T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MOBİL HABERLEŞMEDE ŞİFRELEME ALGORİTMALARI İLE GÜVENLİ KISA MESAJ SERVİSİ UYGULAMASI

ÇAĞATAY TOPAÇ

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Dr. Öğr. Üyesi DERYA ARDA

EDİRNE - 2023

Çağatay TOPAÇ'in hazırladığı "**Mobil Haberleşmede Şifreleme Algoritmaları ile Güvenli Kısa Mesaj Servisi Uygulaması**" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir **Yüksek lisans tezi** olarak kabul edilmiştir.

Jüri Üyeleri:	İmza
Dr. Öğr.Üyesi Cem TAŞKIN	……
Dr. Öğr. Üyesi Derya ARDA (Danışman)	……
Dr. Öğr. Üyesi Halil Nusret BULUŞ	……

Tez Savunma Tarihi: 18/01/2023

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr. Öğr. Üyesi Derya ARDA
Tez Danışmanı ……

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

……

Prof. Dr. Hüseyin Rıza Ferhat KARABULUT
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ YÜKSEK LİSANS PROGRAMI
DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

18 / 01 / 2023
Çağatay TOPAÇ
İmza

Yüksek Lisans Tezi
Mobil Haberleşmede Şifreleme Algoritmaları ile Güvenli Kısa Mesaj Servisi Uygulaması
T.Ü. Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

İletişim teknolojilerinin hızla gelişmesi birçok alanda hayatımızı kolaylaştırırken, diğer yandan da çeşitli haberleşme ortamlarında bilgilerin gizlenmesi ve üçüncü kişilerle paylaşılmaması önem kazanmaktadır. Dijital haberleşmede kullanılacak güvenlik metotları ve şifreleme algoritmaları ile bilginin güvenli bir şekilde korunması ve iletilmesi hedeflenmektedir. Günümüzde en sık kullandığımız haberleşme aracı mobil cihazlardır. Bu cihazlar kablosuz bağlantı sağlayabilme ve taşınabilir olma özelliklerinden dolayı hem iş dünyasında hem sosyal ortamda yaygın olarak kullanılmaktadır.

Günümüzde mobil cihazlarla anlık mesajlaşma uygulamaları sıklıkla kullanılmakla birlikte SMS kısa mesaj servisi de yaygın olarak kullanılmaktadır. SMS hızlı ve internet olmayan durumlarda da kullanılabilen bir haberleşme yöntemidir. Ancak iletilen SMS mesajlarının daha güvenli iletilmesi, istenmeyen üçüncü kişilerden korunma gereği gibi durumlarda şifreleme yöntemlerine başvurmak gerekebilir.

Bu tezde mobil haberleşmede SMS ile gönderilen mesajların siber saldırılara ya da çeşitli saldırılara karşı içeriğinin gizliliği ve bütünlüğünün korunması amacıyla şifreleme yöntemlerinden RSA asimetrik şifreleme ve AES simetrik şifreleme algoritmaları kullanılmıştır. AES şifreleme algoritması ve RSA algoritmasıyla yapılan şifreli SMS gönderimi için Android işletim sisteminde Dart programlama dili ile Flutter SDK'sı 3.7.0-10.0.pre.22 versiyonu kullanılarak mobil uygulama yapılmıştır. Kodlama ve tasarım süreci Visual Studio Code(version 1.74.2) ve Android Studio(version 4.1) programları üzerinde yapılmıştır. Bunun yanı sıra şifreli SMS gönderimi farklı mobil cihazlarda ve sanal cihazlarda test edilmiştir. Yapılan uygulamada farklı anahtar büyüklükleri ve farklı mesaj uzunlukları kullanılarak şifreleme ve şifre çözme süreleri açısından değerlendirilmiştir.

Sonuç olarak tezin temel amacı olan şifreli bir mobil SMS haberleşmesi ile AES ve RSA şifreleme algoritmaları kullanılarak güvenli bir iletişim sağlanabileceği ortaya konmuştur. AES algoritmasıyla gerçekleştirilen uygulama Google play platformunda kullanıcıya sunulmuştur. RSA algoritması gerekli iyileştirmelerden sonra Google play platformunda kullanıcıya sunulması hedeflenmektedir.

Yıl : 2023

Sayfa Sayısı : 66

Anahtar Kelimeler : AES Simetrik Şifreleme, RSA Asimetrik Şifreleme**,** SMS, Flutter-Dart, Mobil Uygulama, Android.

Master's Degree Thesis

Secure Short Message Service Application with Encryption Algorithms in Mobile Communications

Trakya University Institute of Natural and Applied Sciences

Department of Computer Engineering

ABSTRACT

While the rapid development of communication technologies makes our lives easier in many areas, it is also important to hide information in various communication media and not to share it with third parties. It is aimed to protect and transmit information securely with security methods and algorithms to be used in digital communication. Today, the most frequently used communication tool is mobile devices. These devices are widely used in both business and social environments due to their wireless connectivity and portability.

Today, instant messaging applications with mobile devices are frequently used, and SMS short message service is also widely used. SMS is a fast communication method that can be used even when there is no internet. However, it may be necessary to resort to encryption methods in cases such as safer transmission of forwarded SMS messages and protection from unwanted third parties.

In this thesis, RSA asymmetric encryption and AES symmetric encryption algorithms, which are encryption methods, are used in order to protect the confidentiality and integrity of the content of messages sent by SMS in mobile communication against cyber attacks or various attacks. In sending encrypted SMS with RSA algorithm and AES encryption algorithm, a mobile application was made using Dart programming language and Flutter SDK version 3.7.0-10.0.pre.22 in Android operating system. The coding and design process has been done on Visual Studio Code (version 1.74.2) and Android Studio (version 4.1). In addition, sending encrypted SMS has been tested on different mobile and virtual

devices. In the application, it was evaluated in terms of encryption and decryption times by using different key sizes and different message lengths.

As a result, it has been revealed that a secure communication can be provided by using AES and RSA encryption algorithms with an encrypted mobile SMS communication, which is the main purpose of the thesis. The application, which is realized with the AES algorithm, is presented to the user on the Google play platform. It is aimed to present the RSA algorithm to the user on the Google play platform after the necessary improvements.

Year : 2023

Number of Pages : 66

Keywords : AES Symmetric Encryption, RSA Asymmetric Encryption**,** SMS, Flutter-Dart, Mobile Application, Android,

TEŞEKKÜR

Bu çalışmanın tüm aşamalarında her zaman yanımda olup desteğini, bilgisini ve değerli görüşlerini hiçbir zaman esirgemeyen danışmanım Dr. Öğr. Üyesi Derya ARDA'ya teşekkürlerimi bir borç bilirim.

Desteklerini hiçbir zaman esirgemeyen, eğitim hayatım boyunca maddi manevi yanımda olan canım annem Emine, canım ablam Çağla ve manevi desteği için canım yeğenim Aysima'ya sonsuz teşekkür ederim.

İÇİNDEKİLER

ÖZET iv
ABSTRACT vi
TEŞEKKÜR viii
İÇİNDEKİLER ix
ŞEKİLLER DİZİNİ xi
ÇİZGELER DİZİNİ xiii
SİMGELER VE KISALTMALAR DİZİNİ xiv
BÖLÜM 1 1
GİRİŞ 1
BÖLÜM 2 4
KISA MESAJ SERVİSİ (SMS) 4
2.1. Kısa Mesaj Servisi (SMS) Çalışma Prensibi 4
2.2. Kısa Mesaj Servis Merkezi(SMSC) 5
2.3. SMS Güvenliği 6
2.3.1. SMS Güvenliğini Tehdit Eden Unsurlar 6
2.3.2. Şifreli SMS Göndermenin Avantajları 7
BÖLÜM 3 9
ŞİFRELEME ALGORİTMALARI 9
3.1. Kriptoloji Nedir? 9
3.2. Asimetrik Şifreleme Algoritması 9
3.2.1. RSA Asimetrik Şifreleme Algoritması 10
3.2.2. RSA Algoritmasının Matematiksel Yapısı 11
3.3. Simetrik Şifreleme Algoritmaları 13
3.3.1. Gelişmiş Şifreleme Standardı AES Simetrik Şifreleme Algoritması 13
BÖLÜM 4 16
RSA ŞİFRLEME ALGORİTMASI İLE GÜVENLİ SMS MOBİL HABERLEŞME UYGULAMASI 16

4.1. Uygulamada kullanılan Materyal ve Metodlar 17
4.1.1. Mobil Uygulama Gereksinimleri 17
4.1.1.1.Android İşletim Sistemi 17
4.1.1.2.Android Studio ve Mimarisi 17
4.1.1.3. Flutter-Dart 18
4.1.1.4. Kriptografik Kütüphane 19
4.2. RSA İle Şifreli SMS Uygulaması Tasarımı 19
4.3. RSA Algoritması İle Şifreli SMS Mobil Uygulaması ve Analizi 23
4.3.1. Farklı Anahtar Büyüklükleri ile RSA ile SMS Şifreleme-Gönderme-Şifre Çözme Uygulaması 24
4.3.2. RSA Algoritmasıyla Şifreli SMS Gönderme Analizi 30
4.3.3. RSA Algoritmasıyla Şifreli SMS Mobil Uygulama Testlerinin Değerlendirilmesi 34
BÖLÜM 5 36
AES ŞİFRLEME ALGORİTMASI İLE GÜVENLİ SMS MOBİL HABERLEŞME UYGULAMASI 36
5.1. Uygulamada Kullanılan Yazılım Gereçleri ve Metodlar 37
5.1.1. Yazılım Gereksinimleri 37
5.2. AES Algoritması ile Güvenli SMS Mobil Uygulaması 37
5.3. AES Algoritması İle Şifreli SMS Mobil Uygulaması ve Analizi 40
5.3.1. AES -256 Blok Şifreleme ile SMS Şifreleme Uygulaması 41
5.4. AES Algoritması ile Güvenli SMS Gönderme Mobil Uygulama Analizi 42
5.5. AES Algoritması ile Güvenli SMS Gönderme Mobil Uygulama Testlerinin Yorumlanması 43
BÖLÜM 6 45
SONUÇ VE TARTIŞMA 45
KAYNAKLAR 47
ÖZGEÇMİŞ 51
TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER 52

ŞEKİLLER DİZİNİ

Şekil 2. 1. SMS Mimarisi (Peersman vd, 2000) 5
Şekil 2. 2. Şifreli SMS Gönderimi Genel Yapısı 7

Şekil 3. 1. Şifreleme Algoritmaları 9
Şekil 3. 2. Asimetrik Şifreleme Algoritması Şeması. 10
Şekil 3. 3. RSA Algoritmasının Çalışması 11
Şekil 3. 4. Gizli Anahtarlı (Simetrik) Şifreleme Algoritması 13
Şekil 3. 5. AES Algoritmasının İşleyişi 14
Şekil 3. 6. AES Algoritmasının Akış Şeması 15

Şekil 4. 1. Android İşletim Sistemi Mimarisi ve Katmanları (Kılınç,2013) 18
Şekil 4. 2. Flutter'ın Yapısal Çerçevesi (Architecture, 2022) 19
Şekil 4. 3. RSA ile Şifreli SMS Oluşturma Ana Ekran 20
Şekil 4. 4. RSA ile Şifreli SMS Gönderme Ekranı 21
Şekil 4. 5. Kişileri Listeleme Ekranı 22
Şekil 4. 6. Şifreli SMS ile Mesajlaşma Ekranı 23
Şekil 4. 7. 1024 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi 27
Şekil 4. 8. 2048 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi 28
Şekil 4. 9. 3072 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi 29
Şekil 4. 10. (a) 4096 , (b) 8192 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi . 30

Şekil 5. 1. Şifreli SMS-Mesajını Koru İsimli Uygulamanın Google Play Store Görüntüsü 37
Şekil 5. 2. AES -SMS Şifreleme Ana Ekran Görüntüsü 38
Şekil 5. 3. Mesajı Şifreleme Ekranı Görüntüsü 38
Şekil 5. 4. Kişilerim Listesi 39
Şekil 5. 5. SMS Gönderme 39

Şekil 5. 6. Şifre Çözme Ekranı 40

ÇİZGELER DİZİNİ

Çizelge 3. 1. RSA Şifreleme Algoritması ve Örneği 12

Çizelge 4. 1. RSA Algoritmasında Açık ve Gizli Anahtarın Oluşturulma Süreleri..... 26
Çizelge 4.2. Lenovo Intel Core i5 Bilgisayarında Pixel_3a_API_30 emilatörü Sonuçları.. 31
Çizelge 4.3. Lenova Intel Core i5 Bilgisayarında Pixel_3a_XL_API_30 emilatörü Sonuçları 32
Çizelge 4.4 Tekno Spark 6 Go 4 GB RAM ve Android 10 işletim sistemi olan fiziksel telefon ile elde edilen sonuçlar..... 33

Çizelge 5. 1. AES 256, SMS Şifreleme-Şifre Çözme Test Sonuçları..... 43

SİMGELER VE KISALTMALAR DİZİNİ

AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
DOS	Denial of service (Servis Hizmet Reddi)
ECC	Elliptic Curve Cryptography (Eliptik Eğri Kriptolojisi)
FIBS	Federal Information Processing Standards(Federal Bilgi İşleme Standardı)
GPS	Global Positioning System (Küresel Konumlama Sistemi)
GSM	Global System for Mobile Communications (Mobil İletişim İçin Küresel Sistem)
IDE	Integrated Development Environment (Tümleşik Geliştirme Ortamı)
IOS	iPhone Operating System (iPhone İşletim Sistemi)
NIST	National Institute of Standards and Technology **(**Ulusal Standartlar ve Teknoloji Enstitüsü)
RAM	Random Access Memory (Rastgele Erişimli Bellek)
RSA	Rivest-Shamir-Adleman
SMS	Short Message Service (Kısa Mesaj Servisi)
SDK	Software Development Kit (Yazılım Geliştirme Kiti)
SIM	Subscriber Identity Module (Abone Kimlik Modülü)
SMSC	Short Message Service Center (Kısa Mesaj Servisi Merkezi)

.

BÖLÜM 1

GİRİŞ

İletişim teknolojisinin hızla gelişmesi birçok alanda hayatımızı kolaylaştırsa da çeşitli iletişim araçlarında bilgilerin saklanması ve üçüncü kişilerle paylaşılmaması da önemlidir. Cep telefonları, uygulamaya bağlı olarak pratik, hızlı ve taşınabilir özellikleri ile iletişim için kullanılan en popüler cihazlardır. Günümüzde kullanılan akıllı cihazlar, cep telefonları ve tabletler mobil cihazlar olarak adlandırılmaktadır. Günümüzde iletişim için anlık mesajlaşma programları yaygın olarak kullanılsa da kısa mesaj da yaygın olarak kullanılan bir iletişim aracıdır. SMS; Ucuz, hızlı, kullanımı kolay ve internet gerektirmemesi nedeniyle hala iletişim için kullanılan en popüler iletişim yöntemlerinden biridir.

İlk kısa mesaj 30 yıl önce gönderildi. We Are Social 2022 raporuna göre dünya nüfusu 8 milyar civarında olup dünyada, mobil cihaz kullanıcıları sayısı 5.48 milyara ulaşmış ve bugün yaklaşık 5'te 4'ünü akıllı telefonlar oluşturmaktadır.

Dünyada atılan ilk kısa mesaj İngiliz mühendis Neil Papworth ait olup 3 Aralık 1992'de gönderilmiştir. Papworth, meslektaşı Richard Jarvis'e bilgisayardan "Mutlu Noeller" mesajını gönderdi. Her şey gönderilen ilk "Mutlu Noeller" mesajıyla 30 yıl önce başlamış olup Facebook Messenger, iMessage ve WhatsApp gibi yeni, uygulamadan uygulamaya mesajlaşma sunucuları olmasına rağmen metin mesajlaşma hala en yaygın kullanılan cep telefonu mesajlaşma biçimlerinden biri olmaya devam etmektedir (Marketing Türkiye, 2022).

SMS' in GSM üzerinden iletimine baktığımızda SMS mesajın değiştirilmesi, dinlenmesi, tekrar saldırıları ve ortadaki adam saldırılarına maruz kalması olasıdır (Chavan ve Sabness, 2012). Bunun gibi dezavantajlardan dolayı verimli ve hızlı kriptografik şemalar,

güvenilir anahtar yönetimi ve dağıtımı gibi yöntemler ile güvenli SMS iletimi için bir çözüm olabilir. Gizlilik ve bütünlük ilkesi, haberleşme gereken tüm uygulamalarda gerekli olduğu gibi SMS için de önemli bir kıstastır.

Bu tezde SMS mesajının güvenliği ve bütünlüğü için AES şifreleme algoritması ve RSA algoritmasıyla şifreli SMS gönderimi mobil uygulaması gerçekleştirilmiştir. Bunun için Android işletim sisteminde Dart programlama dili ile Flutter SDK'sı kullanılmıştır. Android işletim sistemi, mobil cihazlar ve cep telefonları için geliştirilmiş Linux tabanlı açık kaynaklı bir mobil yazılımdır.

StockApps tarafından paylaşılan bir rapora göre Android işletim sisteminin küresel pazar payının son yıllarda bir miktar düşüş gösterdiğini sunmuştur. Bu rapora göre dünya genelinde 2018'de %77 olan oran, Ocak 2022'de %69'a düşerek %7 'lik bir değer kaybı yaşadı. Bunun yanı sıra iOS'un pazar payı %19'ten %25'e ulaştı ve yaklaşık %6'nın üzerinde artış yaşadı. Ancak yine de kullanım oranlarına göre Andriod işletim sistemi IOS' a göre oldukça fazla pazara sahiptir (Solit net, 2022).

Şifreli SMS için seçtiğimiz AES simetrik şifreleme algoritması günümüzde halen güçlü ve hızlı bir algoritmadır. Donanımsal uygulamalarda kullanışlı ve güvenlidir. Ancak güvenli bir anahtar paylaşımı gereklidir. Bu durum dezavantaj olarak söylenebilir.

RSA asimetrik şifreleme algoritmasıyla şifreli SMS göndermek için tercih edildiğinde yine güvenli, kırılması zor denebilecek güce sahip bir uygulama olması mümkündür. Çünkü RSA algoritmasında seçilen asal sayıların büyük olması şifrelemenin gücünü arttıran durumdur. Ancak bu algoritmada seçilen asal sayıların çok büyük olması fazla işlem gücüne sebep olmaktadır. Dolayısıyla şifreleme ve çözme işlemleri AES'e göre daha yavaştır.

Tez çalışmasında bütünsel açıdan "Mobil Şifreli SMS" kavramı ele alınmıştır. Bu kavram üzerinde yapılan bu tez 6 bölümden oluşmaktadır.

Birinci bölümde tezin amacı, önemi ve literatür açısından özgün değeriyle birlikte giriş yapılmıştır.

İkinci bölümde SMS hakkında temel bilgiler, SMS güvenlik gerekleri, Mobil uygulama tasarım ve ara yüzü bilgileri açıklanmıştır.

Üçüncü bölümde tezde kullanılan RSA asimetrik ve AES simetrik şifreleme algoritmaları üzerinde durulmuştur.

Dördüncü bölümde RSA algoritmasıyla şifreli SMS gönderimi mobil uygulaması ve analizi detaylı bir şekilde anlatılmıştır.

Beşinci bölümde AES algoritmasıyla şifreli SMS gönderimi mobil uygulaması ve analizi anlatılmıştır.

Son olarak altıncı bölümde ise yürütülen tezde RSA algoritmasıyla ve AES algoritmasıyla yapılan şifreli SMS gönderimi mobil uygulamasında farklı anahtar uzunlukları ve mesajın uzunluğu ile ilişkili olarak elde edilen sonuçlar şifreleme ve şifre çözme süreleri açısından değerlendirilmiş ve literatür üzerinden tartışma yürütülmüştür.

Sonuç olarak tezin temel amacı olan şifreli bir mobil SMS haberleşmesi ile ayrı ayrı AES ve RSA şifreleme algoritmaları kullanılarak güvenli bir iletişim sağlanabileceği ortaya konmuş ve AES algoritmasıyla gerçekleştirilen uygulama Google play platformunda kullanıcıya sunulmuştur. RSA algoritması gerekli iyileştirmelerden sonra Google play platformunda kullanıcıya sunulması hedeflenmektedir.

BÖLÜM 2

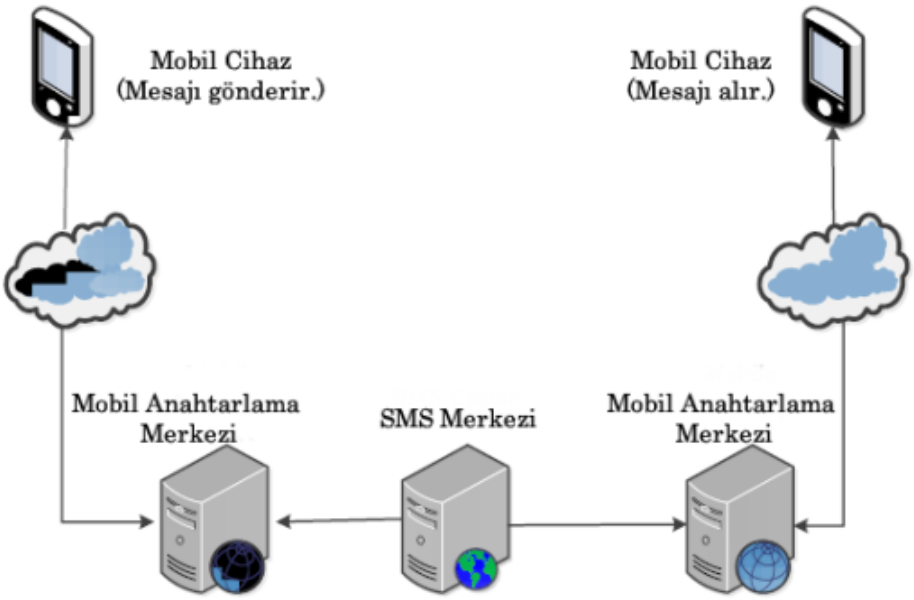
KISA MESAJ SERVİSİ (SMS)

SMS, 1985 yılında mobil iletişim için tanımlanmıştır. SMS "Short Message Service" kısaltmasıdır. Yani "Kısa Mesaj Servisi" dir. SMS; maksimum 160 karakterlik bir mesajı mobil cihaz olan cep telefonundan gönderilmesini sağlayan bir uygulamadır (Peersman vd, 2000).

2.1. Kısa Mesaj Servisi (SMS) Çalışma Prensibi

SMS çoğunlukla cep telefonu servisi olarak kullanılmaktadır. Ancak SIM kart olduğu müddetçe diğer bilgisayar cihazları ile de çalışmaktadır. Şekil 2.1.'de SMS ile mesajlaşma yöntemi incelendiğinde, SMS mesajının alıcıya doğrudan iletilmediği görülmektedir (Peersman vd, 2000, Peersman, Gert vd.2000).

SMS mesajı, önce mesaj yönlendirme işlemini yapan Mobil anahtarlama merkezinden geçer. Daha sonra SMS merkezinde depolanır ve iletim için yönlendirilir (Ariffi vd, 2013).



Şekil 2. 1. SMS Mimarisi (Peersman vd, 2000)

İlk SMS 1992 tarihinde 'Mutlu yıllar' mesajı ile atılmıştır. 1993'de ilk noktadan noktaya çalışan ve sadece SMS alma özelliği olan telefonlar piyasada yer aldı. 1995'de SMS GSM ağlarından gönderilmeye başlanarak uluslararası dolaşım başlamış oldu. 2008'de 4 trilyona yakın SMS gönderilmiştir. 2010 yılında bir yılda 6,1 trilyon SMS gönderilmiştir (ITU 2010, Muştu 2012).

2.2. Kısa Mesaj Servis Merkezi (SMSC)

SMSC, GSM operatörlerinin kısa mesaj trafiğini yöneten merkezdir. SMS mesajı Şekil 2.1'deki gibi önce SMSC' e gelir ve daha sonra alıcı telefonuna gelir (Yüksel ve Zaim, 2009).

2.3. SMS Güvenliği

Her ne kadar anlık mesajlaşma uygulamaları güncelliğini korusa da SMS basitliği ve maliyeti düşük olmasından dolayı uzun süre kullanılacak bir iletişim aracıdır. Ancak GSM ağındaki SMS mesajın değiştirilmesi, dinlenmesi, tekrar saldırıları ve ortadaki adam saldırılarına maruz kalması olasıdır (Chavan ve Sabnees, 2012; Kalenderi vd, 2012). Bunun gibi dezavantajlardan dolayı verimli ve hızlı kriptografik şemalar, güvenilir anahtar yönetimi ve dağıtımı gibi yöntemler ile güvenli SMS iletimi için bir çözüm olabilir. Bu bağlamda tezde RSA ve AES şifreleme algoritmaları ile farklı anahtar büyüklükleri ile mobil cihazlarda şifreli SMS gönderimi çalışılmış ve değerlendirmesi yapılmıştır. Böylece mobil cihazlarda güvenilir bir SMS haberleşmesi sağlanabileceği ortaya konmuştur.

2.3.1. SMS Güvenliğini Tehdit Eden Unsurlar

Ortadaki adam saldırısı (Man-In-Middle Attack): Bu saldırıda SMS trafiğinde yabancı kişinin trafiğe müdahale etmesi söz konusudur. Bu saldırı iletişimin dinlenmesi, değiştirilmesi ve verilerin ele geçirilmesidir.

Böylece kullanıcının hangi sitelere girdiğini, gönderdiği aldığı mailleri, şifreleri gibi bilgilere erişebilir.

Tekrar Saldırıları (Replay Attack): Tekrar saldırısı, kötü niyetli biri kişinin ağ üzerinden geçen veri iletimini ele geçirip bunu tekrarlayarak gerçekleştirdiği bir siber saldırıdır. Yetkili bir kullanıcıdan geldiği düşünüldüğü için ağın güvenlik protokolleri saldırıya normal bir veri geçişi muamelesi yapar.

Mesajı Açığa Çıkarma (Message Disclosure): SMS mesajları alıcıdan önce SMSC' de depolandığı için bu sistemde bulunan kullanıcılar tarafından görüntülenebilir.

Hizmet Aksattırma Saldırıları (Denial of Service-DOS): Bu saldırıda kullanıcının mobil cihazına tekrarlı mesajlar gönderilerek ulaşılmaz hale getirebilmek için yapılmaktadır.

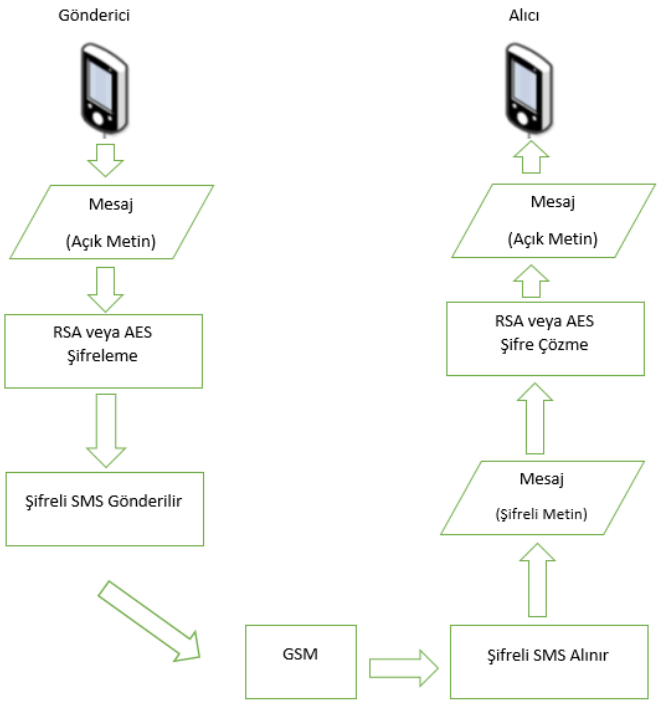
SMS Dinleme: Pasif bir siber saldırı yöntemleridir. Kullanıcının cihazlarına sızarak onları dinleyerek kişisel verilere ulaşmak hedeflenmektedir (Chavan ve Sabnees, 2012).

2.3.2. Şifreli SMS Göndermenin Avantajları

SMS mesajlar gönderici alıcı arasında açık metin olarak iletilir. Bu durumda pek çok istenmeyen durumlarla karşı karşıya kalınabilir. Örneğin;

- Mesaj iletilmeden önce açık metin olarak operatörde tutulur.
- Operatör personeli tarafından okunma olasılığı vardır. Operatör sistemi siber saldırılara maruz kalabilir.

Bu gibi durumlarda güvenli mesajlaşma ortamının sağlanabilmesi için şifreleme algoritmalarından yararlanılabilir. Bu sayede mesaj şifreli olarak iletim ortamında olacaktır. Güçlü ve hızlı şifreleme algoritmaları kullanılarak güvenli mesajlaşma sağlanabilir (Bodur vd, 2015). Şekil 2.2.'de Genel Şifreli SMS gönderimi gösterilmiştir.



Şekil 2. 2. Şifreli SMS Gönderimi Genel Yapısı

Şifreleme yöntemleri gizli ve açık anahtarlı olarak iki kategoride incelenmektedir. Gizli anahtarlı şifrelemede anahtarın gizli, güvenilir bir şekilde iletilmesi gerekir. Bu durum simetrik şifreleme için dezavantajdır (Yayla vd.,2020).

Açık anahtarlı şifreleme olan asimetrik şifrelemede açık ve gizli anahtar vardır. Bu anahtarlar birbirinden farklıdır. Kullanıcının açık anahtarı ile şifrelenmiş veriyi sadece kullanıcının gizli anahtarı çözebilir (Kodaz ve Botsalı, 2010).

Bu tezde, SMS ile güvenli mesajlaşma işlemi için güçlü güvenliğe sahip olan asimetrik şifreleme algoritmalarından biri olan RSA algoritması kullanılmıştır. Ayrıca yine güvenliği kanıtlanmış ve hızlı olan AES simetrik şifreleme algoritmasıyla da şifreli SMS gönderimi gerçekleştirilmiştir. İki algoritma yöntemiyle yapılan şifreli SMS gönderimi için farklı metriklerle testler yapılıp değerlendirilmiştir.

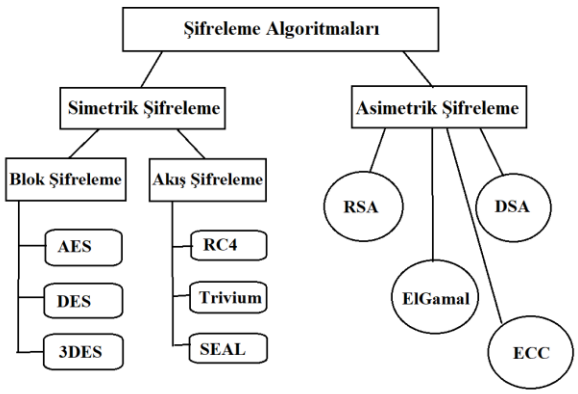
BÖLÜM 3

ŞİFRELEME ALGORİTMALARI

3.1. Kriptoloji Nedir?

Kriptoloji veri güvenliğini sağlayan şifreleme bilimidir. Kriptografi ve kriptanaliz olmak üzere iki alanı içermektedir. Kriptografide şifreleme algoritmaları kullanarak şifreleme yapılmaktadır. Kriptografik algoritmalar gizlilik, veri bütünlüğü, güvenilirlik, erişilebilirlik, kimlik doğrulama ve reddedilemezlik esasları temel almaktadır. Kriptanaliz ise sistemlerin güvenilirlikleri ve zayıf yanlarını inceleyip çözüm bulmaya çalışan daldır (Stinson, 2002).

Şifreleme algoritmaları asimetrik ve simetrik algoritmalar olmak üzere iki kategoride ele alınmaktadır. Aşağıdaki Şekil 3.1.'de bazı şifreleme algoritmaları verilmiştir.

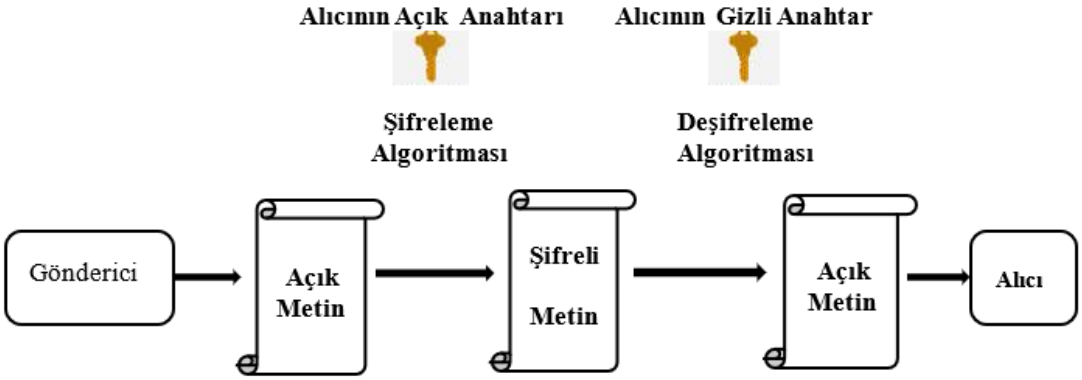


Şekil 3. 1. Şifreleme Algoritmaları

3.2. Asimetrik Şifreleme Algoritması

Asimetrik Şifrelemede, şifreleme işlemi için açık anahtar kullanılırken, şifre çözmede gizli anahtar kullanılır. Bazı asimetrik şifreleme algoritmaları RSA (Rivest, Shamir ve

Adleman, 1978), ECC (Koblitz, 1987) ve Elgamal'dır (Elgamal, 1985). Bu algoritmanın çalışma mantığı Şekil 3.2.'de gösterilmiştir.



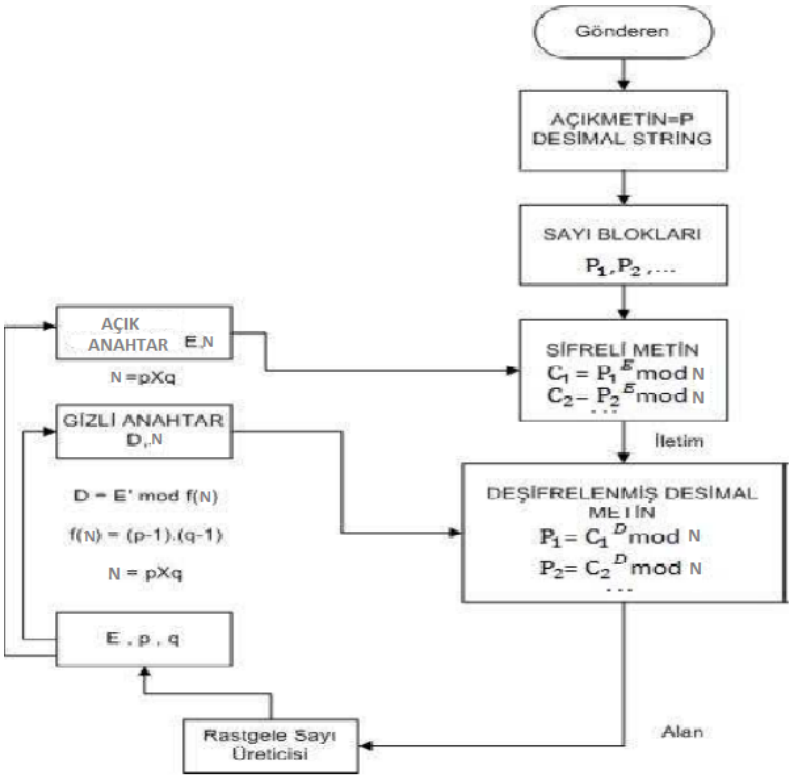
Şekil 3. 2. Asimetrik Şifreleme Algoritması Şeması.

3.2.1. RSA Asimetrik Şifreleme Algoritması

RSA şifreleme sistemi asimetrik şifreleme algoritmalarından olup günümüzde güvenilirliğini korumaktadır. Ron Rivest, Adi Shamir ve Len Adleman tarafından 1977 yılında "A Method for Obtaining Digital Signatures ans Public – Key Cryptosystems" isimli makale ile RSA açık anahtarlı şifreleme algoritması ortaya koyulmuştur. RSA şifreleme algoritması günümüzde güvenilirliğini korumaktadır. RSA Şifreleme Sistemi'nin güvenli olması seçilen asal sayıların büyüklüğü ile doğru orantılıdır. RSA algoritmasında biri açık diğeri gizli anahtar kullanılır. Açık anahtar herkes ile paylaşılabilir. Şifreleme yapacak olan taraf seçilen bu açık anahtar ile bilgiyi şifreler ve alıcı bu şifreli metni ürettiği gizli anahtar ile çözebilir (Rivest, Shamir & Adleman, 1978).

3.2.2. RSA Algoritmasının Matematiksel Yapısı

RSA şifreleme algoritmasında mesaj [0, N-1] arasındaki pozitif tamsayı bloklarına dönüştürülür. Aşağıda Şekil 3.3.'de RSA çalışma adımları gösterilmektedir.



Şekil 3. 3. RSA Algoritmasının Çalışması

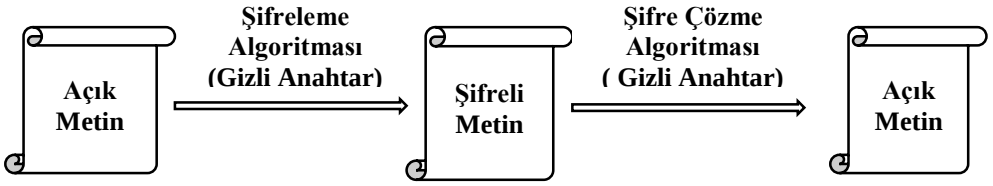
Ayrıca aşağıdaki Çizelge 3.1.'de algoritmanın adımları ve örneği verilmiştir.

Çizelge 3. 1. RSA Şifreleme Algoritması ve Örneği

RSA Algoritması (Anahtar oluşumu, Şifreleme-Deşifreleme	**Örnek**
p ve q asal iki sayı seçilir.	P =23; q=19;
N = **p*q**.	**N** = 23*19 = 437.
Euler's totient fonksiyonu ∅(N) = (**p**-1)(**q**-1).	∅(N) = (23-1) x (19-1) = 22x18 =396
∅(N) değeri ile en büyük ortak böleni 1(aralarında asal) olan rastgele 'e' değeri seçilir..	**e** = 5. (5<396, ve 5 ve 396 nin en büyük ortak böleni 1 dir
e*d = 1 mod ∅**(N)** olacak şekilde d değeri hesaplanır	5***d** = 1 mod 396 => **d** = 317, çünkü 5*317 = 721 = 1 mod 396.
(açık anahtar) public key (**e**, **N**).	Açık anahtar (5, 437).
(gizli anahtar) Private key (**d**, **N**).	Gizli anahtar (317, 437).
Açık metin **M** olsun.	**M** =7 olsun.
Şifreli metin **C** = $\mathbf{M}^{\mathbf{e}}$ mod **N**.	Şifreli Metin **C** = 5^7 mod 437= 215
Şifre çözme işlemi Açık metin =$\mathbf{C}^{\mathbf{d}}$ mod **N** = ($\mathbf{M}^{\mathbf{e}}$) $^{\mathbf{d}}$ mod **N** = **M**.	Açık Metin 215^{317} mod 437 = 7

3.3. Simetrik Şifreleme Algoritmaları

Simetrik algoritmada şifreleme ve şifre çözmek için bir tane gizli anahtar kullanılmaktadır. Kullanılan anahtar gizli olup şifreleme yapan ile şifrelemeyi çözecek kişiler arasında anlaşılmış ortak bir anahtardır (Stinson, 2002). Simetrik şifreleme algoritmalarının çalışma şekli Şekil 3.4.'te gösterilmiştir. En güçlü simetrik algoritmalardan biri AES şifreleme algoritmasıdır.



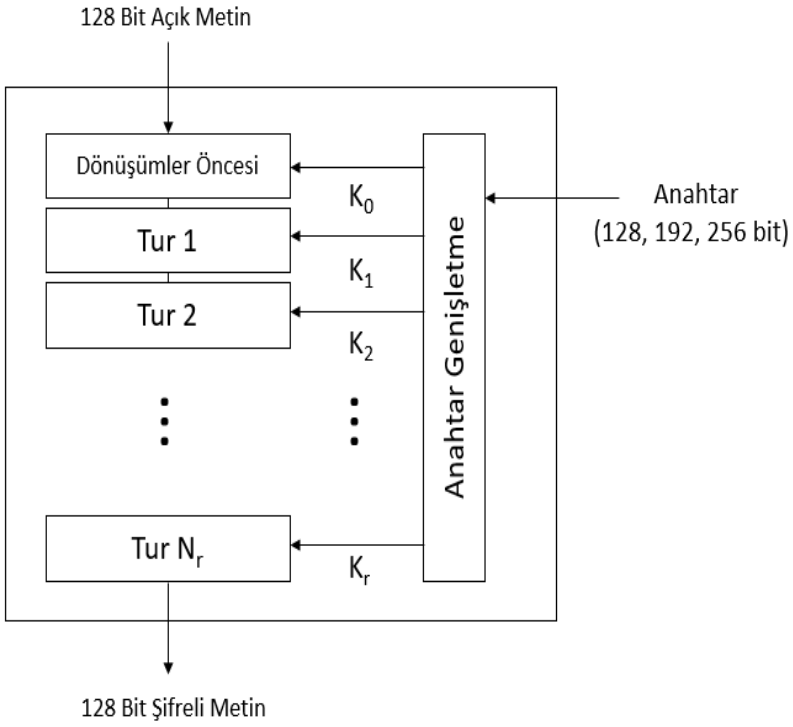
Şekil 3. 4. Gizli Anahtarlı (Simetrik) Şifreleme Algoritması

3.3.1. Gelişmiş Şifreleme Standardı AES Simetrik Şifreleme Algoritması

Günümüzde internetin her alanda kullanılması ile birlikte veri gizliliğinin sağlanması konusu önemini gittikçe arttırmaktadır. Veri gizliliğinde Gelişmiş Şifreleme Standardı AES Algoritması güvenliği halen devam etmekte olan en güçlü simetrik algoritmalardan biridir. Güvenli ve hızlı olması gibi özellikler ön planda tutularak Joan Daemen ve Vincent Rijmen tarafından geliştirilen Rijndael (Daemen & Rijmen,1999) algoritması NIST tarafından gelişmiş kodlama standardı AES olarak seçilmiş ve FIPS olarak yayımlanmıştır (FIPS 197, 2001).

AES algoritması bir blok şifreleme algoritmasıdır. Veriler bloklar şeklinde şifreleme ve şifre çözme işlemlerine alınır. AES uzunluğu 128 bitte sabit olan blok ile uzunluğu 128, 192 ya da 256 bit olan anahtar kullanır (Daemen&Rijmen,2002). AES algoritmasında giriş, çıkış ve matrisler 128 bitliktir. 128 bitlik blok ilk tur öncesinde 4×4'lük matrise dönüştürülür. Aşağıdaki Şekil 3.5'te gösterildiği gibi önce K0 anahtarı ile XOR işlemine sokulur. Daha

sonra her bir turda yapılan işlemler şekil 3.6 da gösterildiği gibidir. Seçilen anahtar boyutu ile ilişkili olarak tur sayıları tamamlanana kadar tur işlemleri tekrar eder. Tur sayısı 128 bitlik anahtar için 10 tur, 192 bitlik anahtar için 12 tur ve 256 bitlik anahtar için 14 turda şifreleme yapılmaktadır. Ancak son turda Şekil 3.5'te gösterildiği gibi sütunların karıştırılması yapılmamaktadır (Demirbilek, 2021; Forouzan,2008; Tüfekçi, 2018).



Şekil 3. 5. AES Algoritmasının İşleyişi

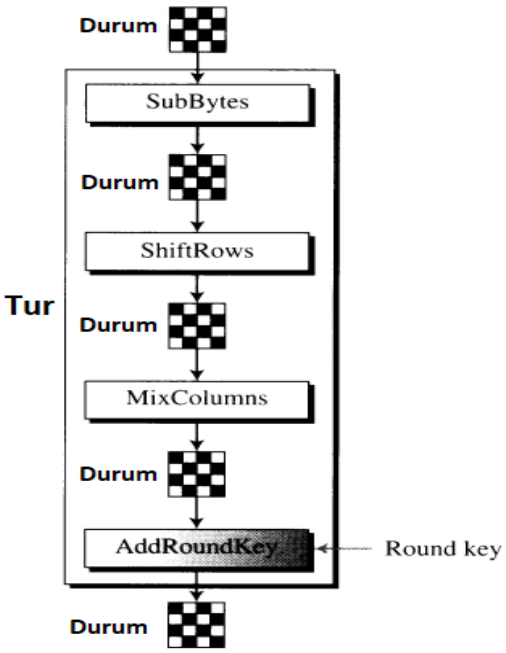
AES'de seçilen anahtar büyüklüğüne göre döngü sayısı değişmektedir. Her bir döngüde birçok aşama vardır.

Her Döngünün Yapısı

1- Tersi alınabilir dönüşümler her döngü için kullanılır.

2- Döngülerde byteların yer değiştirmesi, satırların ötelenmesi, sütunların karıştırılması ve tur anahtarı ile XOR işlemleri şeklinde dört döngü kullanılır. Son döngüde sütunların karıştırılması yapılmaz.
3- Döngülerde kullanılan anahtar, anahtar planlama ile elde edilir.
4- Şifre çözme aşağıdaki adımların tersi sırayla yapılır:
   Sırasıyla ters byte yer değiştirme (InvSubByte), ters satır kaydırma (InvShiftRows), ters sütun karıştırma (InvMixColumns) ve tur anahtarı (AddRounKey) adımları sıraıyla uygulanır.

Şekil 3.6.'de AES'de bir turdaki akış gösterilmiştir. AES algoritmasıyla ilgili daha detaylı bilgiye ve örneklendirmeye Forouzan'nın 2008 yılındaki kitabından ulaşılabilir.



Şekil 3. 6. AES Algoritmasının Akış Şeması

BÖLÜM 4

RSA ŞİFRLEME ALGORİTMASI İLE GÜVENLİ SMS MOBİL HABERLEŞME UYGULAMASI

Son yıllardaki siber silah kullanım amaç ve kullanım alanları yaygınlaşmaktadır. Siber casusluk ve kimlik hırsızlığı gibi bilgisayar korsanları tarafından bilgisayarlarımıza telefonlarımıza sızılıp özel bilgilerimizin, verilerimizin çalınma olasılığı yüksektir. Finans verileri hedef alan bilgisayar korsanları internet kullanıcılarını tedirgin etmektedir. Siber saldırılara karşı alınabilecek korunma yöntemleri gelişen teknolojiye göre zamanla geliştirilip, yeni yöntemler geliştirilmektedir. Bu güvenlik yöntemlerinden biri de kişisel verilerimizi SMS ile haberleşmede korumak istersek burada şifreleme yöntemlerine başvurmaktır.

Bu bölümde mobil cihazlardan yapılan SMS haberleşmesinde RSA şifreleme algoritmasından faydalanılarak güvenli mobil SMS uygulaması anlatılmıştır. Yapılan çalışmada farklı anahtar uzunlukları ve farklı uzunluktaki mesajların şifreleme ve şifre çözme süreleri açısından farklı mobil cihazlarla ve sanal cihazlarda şifreli SMS gönderimi test edilmiştir ve yorumlanmıştır.

4.1. Uygulamada kullanılan Materyal ve Metodlar

4.1.1. Mobil Uygulama Gereksinimleri

Tez çalışmamızda yürütülen uygulamada Android işletim sisteminde Dart programlama dili, Flutter SDK'sı 3.7.0-10.0.pre.22 versiyonu kullanılmıştır. Kodlama ve tasarım için Visual Studio Code(version 1.74.2) ve Android Studio(version 4.1) programları kullanılmıştır.

4.1.1.1.Android İşletim Sistemi

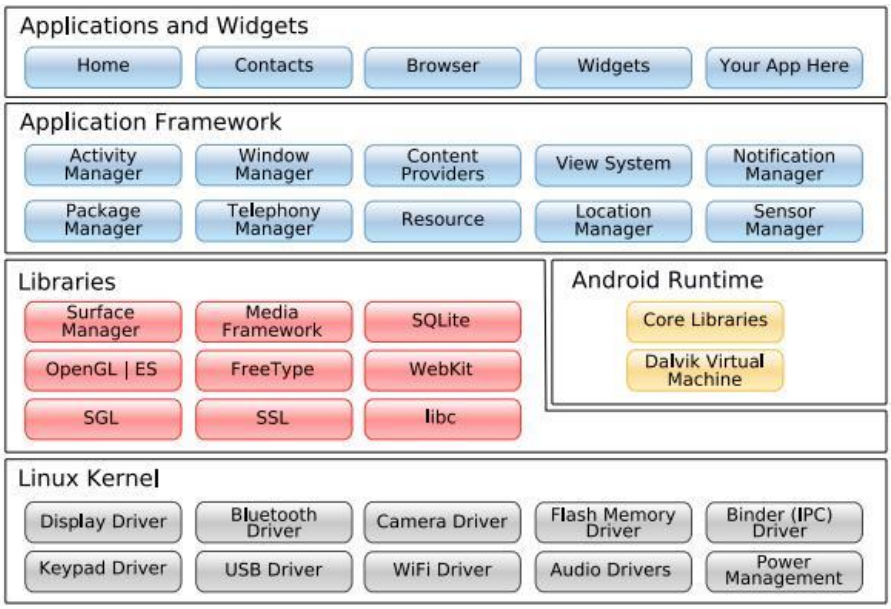
Android, Google ve Open Handset Alliance tarafından, mobil cihazlar için geliştirilmekte olan Linux çekirdeğine sahip açık kaynak kodlu bir işletim sistemidir. Bu özelliğinden dolayı farklı cihazlara uyumlu hale getirilebilmiş ve birçok yerde kullanılmasına olanak sağlamıştır (Open Handset Alliance, 2011).

Android işletim sistemi televizyonlar, notebooklar, akıllı telefonlar, oyun konsolları, akıllı beyaz eşyalar, GPS cihazları gibi birçok cihazlarda kullanılmaktadır (Taç, 2011):

4.1.1.2.Android Studio ve Mimarisi

Android işletim sistemine özgü yazılım Google tarafından derlenmiş Android SDK ile geçekleştirilebilir. Kullanım kolaylığı sunan bir IDE ile geliştirilecek olan yazılımlar, hızlı ve kolay bir şekilde oluşturulabilir. Uygulama geliştirmek için Google'ın oluşturduğu "*http://developer.android.com*" adresi kullanılabilir (Muştu, 2012) (Android, 2011).

Android işletim sisteminde bulunan katmanlar aşağıdaki Şekil 4.1.'de gösterildiği gibidir.



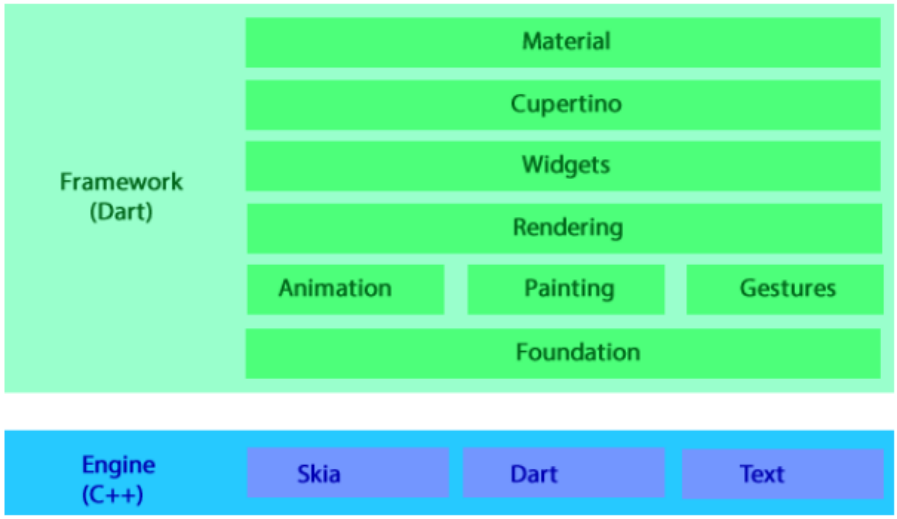
Şekil 4. 1. Android İşletim Sistemi Mimarisi ve Katmanları (Kılınç,2013)

4.1.1.3. Flutter-Dart

Flutter, Google tarafından geliştirilen ve açık kaynak kodlu bir uygulama geliştirmeyi sağlayan SDK (Yazılım Geliştirme Kiti)'dır. Mac, Linux ya da Windows gibi platformlarda sorunsuz çalışması için tasarlanmıştır.

Flutter'da uygulama geliştirmek için Dart programlama dili kullanılmaktadır. Google tarafından 2011'de geliştirilmiş olan Dart, bir nesne programlama dili olarak tanımlanmıştır. Bu dil ile Flutter üzerinden yazılan kodlar platformdan bağımsızdır. Yani hem mobil hem web hem de masaüstü ile uyumlu bir uygulama olmaktadır (Flutter ,2022).

Flutter'ın temel çalışma prensibine bakacak olursak, özel Flutter kütüphanesinde bulunan 'widget' adı verilen nesneler bütün bir ara yüz oluşturulabilmektedir. "Material Design" ve "Cupertino" nesneleri ile uygulamalar, platformdan bağımsız emülatör değiştirilmeden hem Android hem de IOS işletim sistemleri için aynı anda derlenebilir. 100 milyondan fazla açık kaynak projenin paylaşıldığı GitHub'daki popülaritesi ile mobil yazılım geliştiriciler arasında son derece yüksek bir eğilime sahiptir (GitHub, 2020). Şekil 4.2.'de Flutter'ın yapısal çerçevesi verilmiştir (Gülcüoğlu, Üstün ve Seyhan, 2021).



Şekil 4. 2. Flutter'ın Yapısal Çerçevesi (Architecture, 2022)

Flutter'ın gerçek zamanlı önizleme yapılabilmesi, gelişmiş düzgün performansı olan Widget'ler, az kod ile çok yanıt gibi avantajlarını sayabiliriz. Ancak üçüncü taraf kütüphane eksikliği, dosya boyutunun yüksek olması, tek bir yazılım dili olması dezavantaj olarak sayılabilir (Webtekno, 2022).

4.1.1.4. Kriptografik Kütüphane

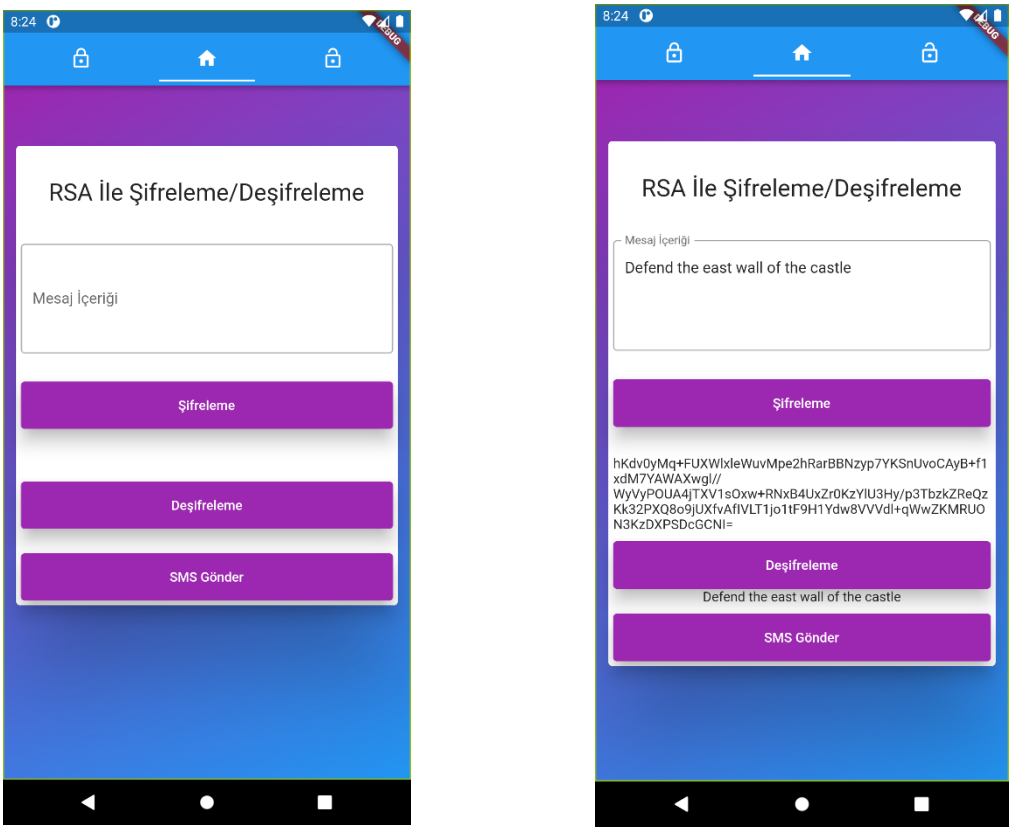
Uygulamada RSA şifreleme için Fast-RSA 3.5.3 kütüphanesi kullanılmıştır(Fast-RSA, 2023).Bu tezde kütüphanedeki anahtar büyüklükleri seçimlere göre kullanılarak anahtara ekleme(padding) yapılmayacak şekilde düzenlenmiştir. Şifreleme, şifre çözme gibi birçok metodu içeren bu kütüphane Dart tarafında kullanılmaktadır.

4.2. RSA İle Şifreli SMS Uygulaması Tasarımı

Uygulama tasarımı genel yapısı aşağıdaki dört ekrandan oluşmaktadır.

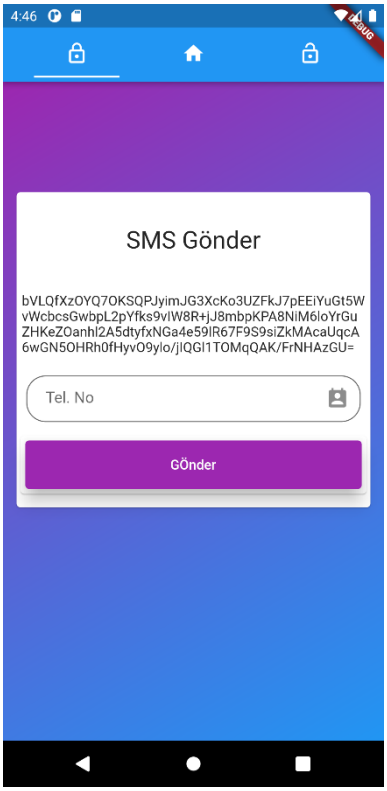
Ana Ekran: Uygulama mağazadan yüklenip açılınca kullanıcının karşısına çıkan ilk ekrandır. Aşağıdaki Şekil 4.3.'de gösterildiği gibi mesaj içeriği girildikten sonra şifreleme

işlemi yapılabilmektedir. Deşifreleme butonu ile mesaj görüntülenebilmektedir. SMS Gönder butonu kullanıcıyı SMS Gönder ekranına yönlendirmektedir.



Şekil 4. 3. RSA ile Şifreli SMS Oluşturma Ana Ekran

SMS Gönder Ekranı: Şifrelenen mesajın SMS atmak için kullanılan Şekil 4.4.'deki ekrandır. Şifreli SMS göndermek için Kişileri Listele Ekranı kullanılır ve sonrasında Gönder butonuna basınca SMS ekranına yönlendirilir.

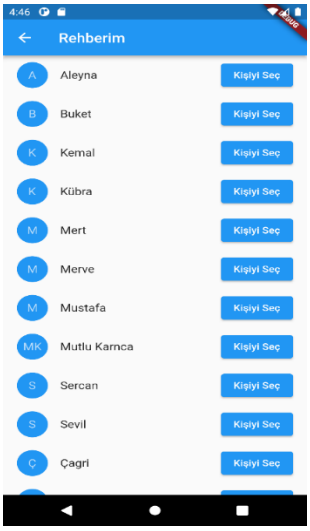


Şekil 4. 4. RSA ile Şifreli SMS Gönderme Ekranı

Kişileri Listeleme Ekranı: Telefon rehberinde bulunan kişilerin tek seferlik izinle çekilip listelendiği ekrandır. Daha sonra bu izinle çekilen numaralar ekranda Şekil 4.5.'deki gibi listelenmektedir. Bunun için yürütülen kod kısmı aşağıda verilmiştir.

Rehberdeki kişileri listelemek için alınan izin kod kısmı:

```
     Future<PermissionStatus> _getPermission() async {
    PermissionStatus permission = await Permission.contacts.status;
    if (permission != PermissionStatus.granted &&
        permission != PermissionStatus.permanentlyDenied) {
      PermissionStatus permissionStatus = await
Permission.contacts.request();
      return permissionStatus;
    } else {
      return permission;
    }
  }
```

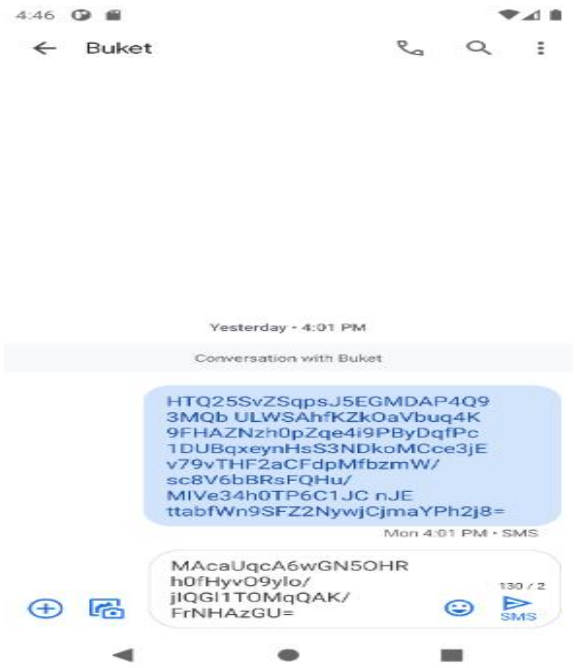


Şekil 4. 5. Kişileri Listeleme Ekranı

Şifreli SMS Mesajlaşma Ekranı: Şekil 4.6'de gösterildiği gibi bu ekranda gereken SMS'i göndermektir. Gönder işleminden sonra RSA ile şifreli mesaj gönderilmiştir. Aşağıda bunun için yürütülen kod kısmı verilmiştir.

SMS Gönderimi

```
sms1 =
"sms:{widget.phoneNumbers.toString()}?body=${widget.message.toString()}";
launch(sms1.toString());
```



Şekil 4. 6. Şifreli SMS ile Mesajlaşma Ekranı

4.3. RSA Algoritması İle Şifreli SMS Mobil Uygulaması ve Analizi

Bu bölümde, farklı anahtar uzunlukları kullanılarak RSA asimetrik şifreleme algoritması ile SMS mesajını şifreleme, gönderme ve şifre çözme mobil uygulaması gerçekleştirilmiştir. Ayrıca farklı mesaj uzunlukları ile kullanılan anahtar büyüklüğüne göre şifreleme ve şifre çözme süreleri farklı emülatörde ve fiziksel telefonda test edilerek yorumlanmıştır.

4.3.1. Farklı Anahtar Büyüklükleri ile RSA ile SMS Şifreleme-Gönderme-Şifre Çözme Uygulaması

Şifreli olarak gönderilmek istenen mesaj “Defend the east wall of the castle” olsun. Boşluklarla birlikte 34 karakterden oluşmaktadır.

1024 bitlik iki asal sayıdan RSA anahtarı üretilmesi kod kısmı

```
//Anahtarı üretme kısmı
 void generate() async {
  try {
    keyPairr = await RSA.generate(1024); //1024, 2048, 3072, 4096, 8192
    setState(() {

       keyPairr = keyPairr;
       print(keyPairr);

    });

  } catch (e) {
    print(e);
  }
}
```

RSA için 1024 bitlik anahtar üretimi ile elde edilen açık ve gizli anahtar aşağıdaki gibidir.

Private Key (Gizli Anahtar)

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDBKCjcUgoa8gTwV4ik+QDoAHW10rf2TAUnieZOqBuXkAsV06+
U 5Y0rUxpXdmhPWfPHoCttVZFk5Zpksdlyg9aJ3Dx2nIpgfWXDEdmCiWKKQb8KKhTI
3RywmoaCkIMYD1CIEjbqDZsn7PumhReBsemPb1MACfkLNpuife9kxpEZ4wIDAQAB
AoGAR/qVL3UK+vuRR5b2/rMj2VDCjJ0XnJq7mP5Uap9OmO4+k0WtOolIUArJ2Cnx
uRBGPe+7/yRR6A1/uWJlK71hZpwJGHnYarepf4yC0kkvvKqKBcnJIpJwXVXt81gI
ICWRGDBOUdEkN22PvlTp7eW29cEMsa2FyEOPzc6J0+TERfECQQDwHQvfIuVBlYH
K y7eL7VNPuyE3PD5x9/GI769rPN+iszRhexaWXNFPrkYuXu0g8zHv0rw9VELh9RAt
Gjp9l0aNAkEAze/Hn+XEUNa9yW3zHc5hCiNv+/oPPAFMIxonwmOsh7AdJYBz5LMr
LYxQQH7l3wFFvrR1lpoyli+FBUI9cMk+LwJBAO9lNlnhk8tgwYgstjJniyG6Q/Kr
OOMuPn214yK7DYlMvJPYQfvmTLXx3n0LHcc1UXt3k0BeS1S3ncoqFVj0Q10CQQCR
Y0MPw+sBF1oNpy4IUPd5bONWhYfT2SajcYe4WR4o/VDWdQVc5JELKxBNOEmZUx
Cm Pkj19g7YsNu8hrNRuQHJAkBmDcmxJu11Bsa5aLY7kP1lSUCh9qw09yvbvlFAs0/M
68N7hZtUxm8wJgUxQhDOyVrcG12kB4akk1JLYgNbnOpG -----END RSA PRIVATE
KEY-----

Public Key(Açık Anahtar)

-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMEoKNxSChryBPBXiKT5AOgAdbXSt/ZMBSeJ5k6oG5eQCxXTr5TljStT
Gld2aE9Z88egK21VkWTlmmSx2XKD1oncPHacimB9ZcMR2YKJYopBvwoqFMjdHLCa
hoKQgxgPUIgSNuo

RSA şifreleme algoritmasında kullanılan anahtarların üretilme süreleri farklı anahtar uzunlukları için aşağıdaki Çizelge 4.1.'de verilmiştir

Çizelge 4. 1. RSA Algoritmasında Açık ve Gizli Anahtarın Oluşturulma Süreleri

Rsa Anahtar Uzuınluğu(bit)	Emülatörde (sn)	Fiziksel Telefonda (sn)
1024	0.057676	0.037358
2048	0.068867	0.041008
3072	0.130958	0.043347
4096	0.228468	0.043764

Seçilen farklı şifreleme anahtarı büyüklüğüne göre RSA algoritmasıyla yapılan SMS şifrelemesi için kod bölümü aşağıdaki gibidir. Şekil 4.7.'de 1024 bitlik anahtar ile yapılan RSA algoritmasıyla şifreli SMS gönderim ekran görüntüsü verilmiştir.

RSA ile SMS Şifreleme Kod Kısmı

```
static Future<String> encrypt(
      String message, String label, Hash hash, String publicKey) async {
    var requestBuilder = model.EncryptRequestObjectBuilder(
      message: message,
      label: label,
      publicKey: publicKey,
      hash: model.Hash.values[hash.index],
    );

    return await _stringResponse("encrypt", requestBuilder.toBytes());
  }
```

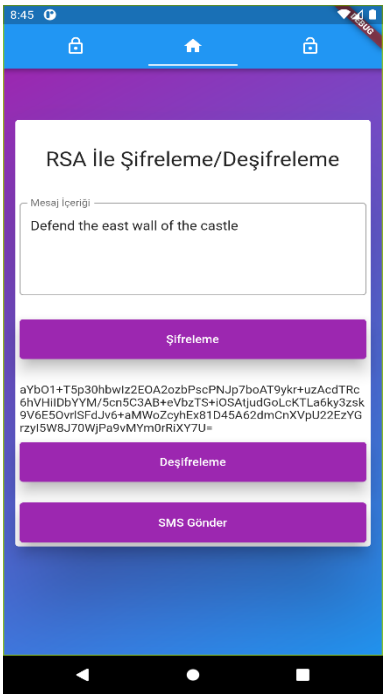
Şifreli SMS:

aYbO1+T5p30hbwIz2EOA2ozbPscPNJp7boAT9ykr+uzAcdTRc6hVHiIDbYYM/5cn5C3
AB+eVbzTS+iOSAtjudGoLcKTLa6ky3zsk9V6E5OvrlSFdJv6+aMWoZcyhEx81D45A62d
mCnXVpU22EzYGrzyI5W8J70WjPa9vMYm0rRiXY7U=

RSA ile SMS'in Şifre Çözme Kod kısmı

```
//Deşifreleme Kısmı
  static Future<String> decryptOAEP(
      String ciphertext, String label, Hash hash, String privateKey) async {
    var requestBuilder = model.DecryptOAEPRequestObjectBuilder(
      privateKey: privateKey,
      ciphertext: ciphertext,
      label: label,
      hash: model.Hash.values[hash.index],
    );

    return await _stringResponse("decryptOAEP", requestBuilder.toBytes());
  }
```



Şekil 4. 7. 1024 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi

```
keyPairr = await RSA.generate(2048);
```

Yukarıda kod parçası verilen Şekil 4.8.'de uygulama arayüzünde gösterilen 2048 bitlik üretilen açık ve gizli anahtar için şifreli SMS metni aşağıdaki gibidir.

Şifreli SMS:

d3PTs0feS/wPncMfLi5Ow/tLxoeTE4HOUkzaM4IMXqyPHDpSAL6lQN6HmPoRLU1BO
D1AwtWNVtvaqiSiWMX9heHbTZaa8vTrZLvoGSzMDIEBiS2hP8pkqaQ8vRjJbooU/2m
ApATgTI9nSbmCcTrhiNEZfoPFb4xmcd3qM7mQrIVzAuzE9Hk6iDDN7cTwm4nN8K01
WkKO5vWRbnnbRpLvOtn6fYhmMIbolONPRAT1mTWu/EO8tK1ez0p/PODfb5HfY5Nk
j4rGdRAyCb4sEiYHcGas1VU9mvUIlbZoVWouKlcHnKbeWLP/Vx/KJY/heFkSmUkylW
rX8SgoRe4rTRLaHA==

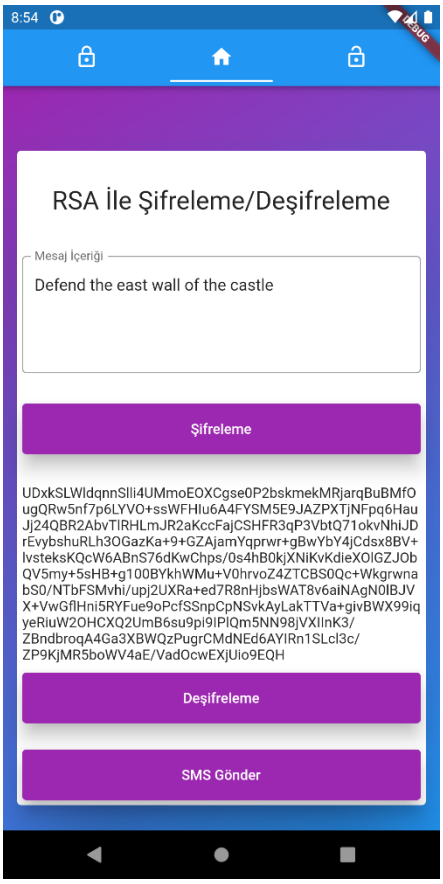


Şekil 4. 8. 2048 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi

```
keyPairr = await RSA.generate(3072);
```

3072 bitlik üretilen anahtarlara göre şifrelenen SMS mesajı aşağıdaki gibidir ve Şekil 4.9.'de ekran görüntüsü verilmiştir.

UDxkSLWldqnnSlli4UMmoEOXCgse0P2bskmekMRjarqBuBMfOugQRw5nf7p6LYVO+ssWFHIu6A4FYSM5E9JAZPXTjNFpq6HauJj24QBR2AbvTlRHLmJR2aKccFajCSHFR3qP3VbtQ71okvNhiJDrEvybshuRLh3OGazKa+9+GZAjamYqprwr+gBwYbY4jCdsx8BV+lvsteksKQcW6ABnS76dKwChps/0s4hB0kjXNiKvKdieXOlGZJObQV5my+5sHB+g100BYkhWMu+V0hrvoZ4ZTCBS0Qc+WkgrwnabS0/NTbFSMvhi/upj2UXRa+ed7R8nHjbsWAT8v6aiNAgN0lBJVX+VwGflHni5RYFue9oPcfSSnpCpNSvkAyLakTTVa+givBWX99iqyeRiuW2OHCXQ2UmB6su9pi9IPlQm5NN98jVXIInK3/ZBndbroqA4Ga3XBWQzPugrCMdNEd6AYIRn1SLcl3c/ZP9KjMR5boWV4aE/VadOcwEXjUio9EQH

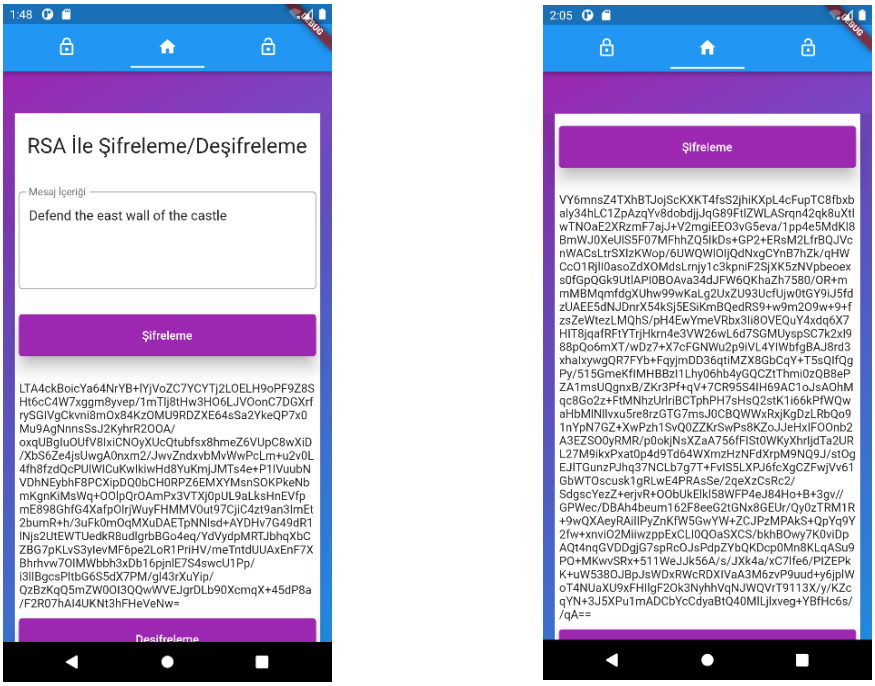


Şekil 4. 9. 3072 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi

```
keyPairr = await RSA.generate(4096);
```

```
keyPairr = await RSA.generate(8192);
```

4096 ve 8192 bitlik üretilen anahtarlara göre şifrelenen SMS mesajı Şekil 4.10.'de verilmiştir.



(a) (b)

Şekil 4. 10. (a) 4096 , (b) 8192 Bitlik Anahtar İle SMS Mesajının RSA İle Şifrelenmesi

4.3.2. RSA Algoritmasıyla Şifreli SMS Gönderme Analizi

Farklı uzunluklarda alınan SMS mesajı için farklı emülatör ve fiziksel telefonda elde edilen test sonuçları Çizelge 4.2'de, Çizelge 4.3'de ve Çizelge 4.4'de verilmiştir.

34 Karakterlik SMS Mesajı : "Defend the east wall of the castle"

66 Karakterlik SMS Mesajı: "Contrary to popular belief, Lorem Ipsum is not simply random text"

124 Karakterlik SMS Mesajı: "It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout"

185 Karakterlik SMS Mesajı: “Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy”

Lenova Intel Core i5 bilgisayarında oluşturulan Pixel_3a_API_30 emilatörü ile elde edilen SMS mesajını şifreleme/şifre çözme süreleri aşağıdaki Çizelge 4.2.’de verilmiştir.

Çizelge 4.2. Lenova Intel Core i5 Bilgisayarında Pixel_3a_API_30 emilatörü Sonuçları

Anahtar Uzunluğu (bit)	Mesaj Boyutu (byte)	Şifreleme (sn)	Şifre Çözme (sn)
1024	34	1.3261	1,0673
	66	1,3866	1.2423
	124	1.5131	1.2931
	185	1.8166	1.3654
2048	34	1,4443	13222
	66	1.7809	1.3522
	124	1.7948	1.5240
	185	1.9551	1.7191
3072	34	1.4950	1,3808
	66	1,6771	1.5888
	124	2.0582	1.6979
	185	2.2358	1.9105
4096	34	1,5922	1,5005
	66	1.9995	1.5349
	124	2.2431	1.6185
	185	2.3784	1.6616
8192	34	1.9852	1,8827
	66	2.5685	2.5321
	124	2.8341	2.7379
	185	2,9354	2.9059

Lenova Intel Core i5 bilgisayarında oluşturulan Pixel_3a__XL_API_30 emilatörü ile elde edilen SMS mesajının şifreleme/şifre çözme süreleri aşağıda Çizelge 4.3.'de verilmiştir.

Çizelge 4.3. Lenova Intel Core i5 Bilgisayarında Pixel_3a_XL_API_30 emilatörü Sonuçları

Anahtar Uzunluğu (bit)	Mesaj Boyutu (byte)	Şifreleme (sn)	Şifre Çözme (sn)
1024	34	1,5637	1,1838
	66	1.7121	1.3801
	124	1.8011	1.4892
	185	1.9372	1.6037
2048	34	1,6521	1,4291
	66	1.6564	1.4693
	124	1.9307	1.6984
	185	2.1864	2.0068
3072	34	1,6727	1.4397
	66	1.7186	1,4842
	124	1.8871	1.5116
	185	2.37591	1.8661
4096	34	1,7475	1.4849
	66	1.9249	1,7492
	124	2.0159	1.9740
	185	2.3323	2.2915
8192	34	1,9721	1,8351
	66	1.9487	1.8891
	124	2.4804	2.2773
	185	2.6091	2.5424

Çizelge 4.4.'de Tekno Spark 6 Go 4 GB RAM ve Android 10 işletim sistemi ve Çizelge 4.5'de Samsung Galaxy A2 1 GB RAM ve Motorola Moto E4 Android Sürümü 7.1.1 RAM 3 GB fiziksel telefon ile elde edilen sonuçlar verilmiştir.

Çizelge 4.4 Tekno Spark 6 Go 4 GB RAM ve Android 10 işletim sistemi olan fiziksel telefon ile elde edilen sonuçlar

Anahtar Uzunluğu (bit)	**MesajBoyutu (byte)**	**Şifreleme (sn)**	**Şifre Çözme (sn)**
1024	34	0.7490	0.7580
	66	0,8374	0.8676
	124	0.8700	0,8944
	185	0.8750	0.9281
2048	34	0.8227	0.8486
	66	0.8547	0.8699
	124	0,8857	0.8926
	185	0.9956	0,9984
3072	34	0.8409	0.8958
	66	0,9051	0.9149
	124	0.9170	0,9531
	185	0.9500	0.9669
4096	34	0.8718	0.9696
	66	0.9125	0,9732
	124	0,9185	1.1058
	185	0.9593	1.1798
8192	34	0.8925	1,0035
	66	0.9646	1.3477
	124	0,9758	1.4116
	185	0.9982	1.5441

Çizelge 4. 5. Motorola Moto E4 ve Samsung Galaxy A2 olan fiziksel telefon ile elde edilen sonuçlar

		Motorola Moto E4		Samsung Galaxy A2	
Anahtar Uzunluğu (bit)	**MesajBoyutu (byte)**	**Şifreleme (sn)**	**Şifre Çözme (sn)**	**Şifreleme (sn)**	**Şifre Çözme (sn)**
1024	34	0.6394	0.6563	0.6277	0.6465
	66	0.6819	0.7421	0.6308	0.6919
	124	0.8241	0.8506	0.7171	0.7451
	185	0.9670	0.9891	0.7979	0.8218
2048	34	0.6912	0.7002	0.6960	0.7133
	66	0.7643	0.7823	0.7379	0.7536
	124	0.8814	0.9070	0.7493	0.8469
	185	0.9923	1.0044	0.8577	0.9710
3072	34	0.7665	0.8137	0.7481	0.8137
	66	0.8951	0.9031	0.8731	0.9438
	124	0.9794	1.0021	0.9645	0.9965
	185	1.0049	1.0141	0.9920	1.0013
4096	34	0.7802	0.9973	0.8143	0.8300
	66	0.9441	1.0014	0.8964	0.9837
	124	0.9969	1.0584	0.9987	1.0088
	185	1.1025	1.2504	1.0952	1.1218
8192	34	0.8201	1.0087	0.8315	0.9801
	66	0.9845	1.1254	0.9708	1.1159
	124	1.0102	1.3602	1.1145	1.3241
	185	1.2230	1.5200	1.2802	1.6455

4.3.3. RSA Algoritmasıyla Şifreli SMS Mobil Uygulama Testlerinin Değerlendirilmesi

Gerçekleştirilen uygulama, SMS'i şifreleme ve çözme süreleri sanal cihazlarda fiziksel cihazlara göre daha yavaştır. Tabi bu kullanılan bilgisayarın, telefonun özelliklerine göre değişebilmektedir. Çizelge 4.4. ve 4.5.'de gösterildiği gibi kullanılan fiziksel cihaz yani akıllı telefonların özelliklerine göre şifreli SMS gönderimi hızlı ve güvenilir olduğunu söylemek mümkündür. Dolayısıyla bir mobil cihaz ile güvenli bir SMS ile haberleşme yapma

gereği olduğunda RSA algoritmasından faydalanılabileceği söylenebilir. RSA algoritmasındaki güvenlik seçilen anahtarın büyüklüğü ile doğru orantılıdır. Çünkü anahtar oluşturmak için seçilen asal sayıların büyük olması saldırganlar için anahtarı elde etmedeki zorlukla sonuçlanır. Şu anki teknoloji ile şifreli SMS haberleşme esnasında mesajın kırılması mümkün gözükmemektedir. Gelecekte kuantum bilgisayarlar ile birlikte olası bir durum olsa bile bu teknolojilere karşı korunmak için kuantum kriptografi de gelişmektedir.

Ancak şöyle bir sorun ortaya çıkmaktadır. SMS mesajlaşma servisi sadece 160 karakterle sınırlı olduğu için şifreleme sonucu elde edilen mesaj daha fazla karakterde olmaktadır. Bu durumda mesajı bölerek göndermek ya da sıkıştırma algoritmalarından faydalanmak gerekebilir.

BÖLÜM 5

AES ŞİFRLEME ALGORİTMASI İLE GÜVENLİ SMS MOBİL HABERLEŞME UYGULAMASI

Simetrik şifreleme algoritması olan AES algoritması hızlı, güçlü ve güvenilirliği kanıtlanmış olmasından dolayı donanımsal ve yazılımsal uygulamalarda kullanmanın avantajlı olduğu söylenebilir. Ancak anahtar dağıtım problemi simetrik algoritmaların dezavantajıdır (Daemen&Rijmen,2002).

Bu bölümde uygulamada SMS mesajını güvenli iletmek için simetrik şifreleme algoritması olan AES-256 bit anahtar uzunluklu blok şifreleme algoritması kullanılmıştır. Ve analizi yapılıp değerlendirilmiştir.

Ayrıca yapılan bu uygulama Google Play Store üzerinde yayınlanıp kullanıcıların deneyimine sunulmuştur (Arda ve Topaç, 2020).

5.1. Uygulamada Kullanılan Yazılım Gereçleri ve Metodlar

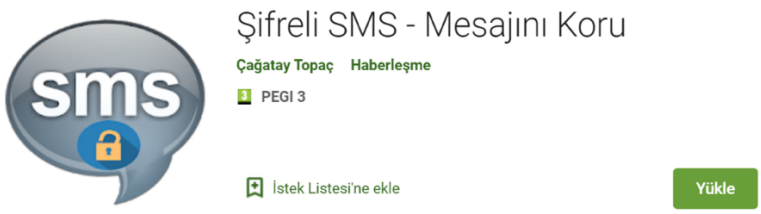
5.1.1. Yazılım Gereksinimleri

Bu bölümde de bölüm 4'te anlatıldığı gibi AES algoritmasıyla SMS mesajını şifreli gönderme-alma-çözme için aynı uygulama gereksinimleri kullanılmıştır. Tekrar edersek bu uygulama da Android işletim sisteminde Dart programlama dili kullanılarak Flutter SDK'sı 3.7.0-10.0.pre.22 versiyonu ile yazılmıştır. Kodlama ve tasarım süreci Visual Studio Code (version 1.74.2) ve Android Studio (version 4.1) programları üzerinde yapılmıştır.

5.2. AES Algoritması ile Güvenli SMS Mobil Uygulaması

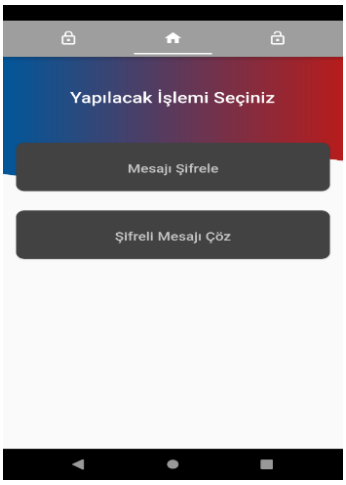
Uygulamanın aşamaları şu şekildedir. Birinci aşamada uygulama açıldığında çıkan ana ekrandır. İkinci aşama SMS mesajını AES ile şifreleme ekranıdır. Üçüncü aşamada rehberdeki kişilerin listelendiği ekrandır. Dördüncü aşama ise AES ile şifreli mesaj göndermedir. Beşinci aşamada ise şifre çözme işlemlerinin yapıldığı bölümdür

Sonuçlanan uygulama Google Play Store üzerinde yayınlanmış olup, kullanıcıların deneyimine sunulmuştur. Bu mobil uygulamamızın genel görüntüsü aşağıdaki Şekil 5.1.'de gösterildiği gibidir.



Şekil 5. 1. Şifreli SMS-Mesajını Koru İsimli Uygulamanın Google Play Store Görüntüsü

SMS Ana Ekran: SMS mesajının AES ile şifreleme ve çözme uygulaması Şekil 5.2.'de verildiği gibi ana ekranıdır.



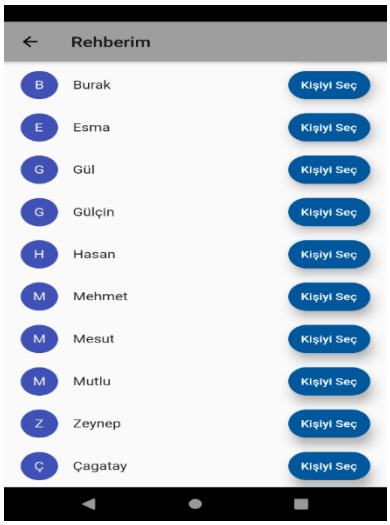
Şekil 5. 2. AES -SMS Şifreleme Ana Ekran Görüntüsü

SMS Mesajını Şifrelemek Ekranı: SMS bilgilerinin girilip, mesajın AES ile şifrelendiği Şekil 5.3.'de gösterilen ekrandır.



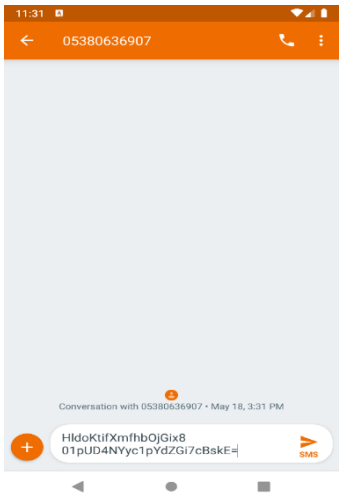
Şekil 5. 3. Mesajı Şifreleme Ekranı Görüntüsü

Kişilerim Listesi: Telefon rehberindeki kişilerin listelendiği ekrandır. Burada kişilerime erişmek için kullanıcıdan tek seferlik bir izin istenip Şekil 5.4.'deki gibi listelenmektedir.



Şekil 5. 4. Kişilerim Listesi

SMS Gönder Ekranı: Bu ekranda Şekil 5.5.'de gösterildiği gibi şifreli SMS gönderilmektedir



Şekil 5. 5. SMS Gönderme

Şifre Çözme Ekranı: Gelen şifreli SMS mesajını çözme ekranı Şekil 5.6.'da verilmiştir.



Şekil 5. 6. Şifre Çözme Ekranı

5.3. AES Algoritması İle Şifreli SMS Mobil Uygulaması ve Analizi

Bu bölümde, farklı anahtar uzunlukları kullanılarak AES simetrik şifreleme algoritması ile SMS mesajını şifreleme, gönderme ve şifre çözme mobil uygulaması gerçekleştirilmiştir. Ayrıca farklı mesaj uzunluklarını şifreleme ve şifre çözme süreleri farklı emülatörde ve fiziksel telefonda test edilerek yorumlanmıştır.

5.3.1. AES -256 Blok Şifreleme ile SMS Şifreleme Uygulaması

AES 256 ile SMS şifreleme için kullanılan kod kısmı aşağıda verilmiştir.

AES İle Sms'i Şifreleme Kod Kısmı

```
    void encDec(String tel, String message, String password) {
      if (password.length < 32) {
        int length = 32 - password.length;
        for (var i = 0; i < length; i++) {
          password = password + '.';
        }
      }

      final key = encrypt.Key.fromUtf8(password);
      final iv = encrypt.IV.fromLength(16);
      final encrypter = encrypt.Encrypter(encrypt.AES(key));
      message = replaceMyChars(message);

      final encrypted = encrypter.encrypt(message, iv: iv);
      print(encrypted.base64);


if (password.length < 32) {
      int length = 32 - password.length;
      for (var i = 0; i < length; i++) {
        password = password + '.';
      }
    }

    try {
           var decrypted = encrypter.decrypt64(encrypted.base64, iv: iv);
    } catch (e) {
      print("hata1");
    }




      String sms1 = "sms: $tel?body=${encrypted.base64}";
      launch(sms1);
    }
```

Şifreli Gelen Sms Mesajinin AES ile Deşifreleme Kod Kismi

```
void encDec(String message, String password) {
  if (password.length < 32) {
    int length = 32 - password.length;
    for (var i = 0; i < length; i++) {
      password = password + '.';
    }
  }
  final key = encrypt.Key.fromUtf8(password);
  final iv = encrypt.IV.fromLength(16);
  final encrypter = encrypt.Encrypter(encrypt.AES(key));
  try {
    var decrypted = encrypter.decrypt64(message, iv: iv);
    print(decrypted);
    _showMessageDialog(decrypted);
  } catch (e) {
    print("hata1");
    _showMyDialog();
  }
}
```

5.4. AES Algoritması ile Güvenli SMS Gönderme Mobil Uygulama Analizi

Farklı uzunluklarda alınan SMS mesajı için farklı emülatör ve fiziksel telefonda elde edilen test sonuçları Çizelge 5.1'de verilmiştir. Kullanılan mesajlar aşağıdaki gibi olsun.

34 Karakterlik Mesaj Uzunluğu:" Defend the east wall of the castle"

66 Karakterlik Mesaj Uzunluğu: "Contrary to popular belief, Lorem Ipsum is not simply random text"

124 Karakterlik Mesaj Uzunluğu: "It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout"

185 Karakterlik Mesaj Uzunluğu: “Many desktop publishing packages and web page editors now use Lorem Ipsum as their default model text, and a search for 'lorem ipsum' will uncover many web sites still in their infancy”

Çizelge 5. 1. AES 256, SMS Şifreleme-Şifre Çözme Test Sonuçları

Cihaz Adı	Mesaj Boyutu	Şifreleme Süresi (sn)	Şifre Çözme Süresi(sn)
Pixel_3a_API_30_x86	34	0,06718	0,03563
	66	0.06997	0.04013
	124	0.08670	0.04359
	185	0.09043	0.04741
Pixel_3a_XL_API_30_x86	34	0.05524	0.03189
	66	0.06044	0.03316
	124	0.06102	0.03507
	185	0.07487	0.04487
Tekno Spark 6 Go	34	0.00323	0.00494
	66	0.00451	0.00638
	124	0.00763	0.00959
	185	0.00969	0.01252

Çizelge 5.1.’deki verilere göre SMS mesajının AES -256 blok şifreleme algoritması ile güvenli ve hızlı bir şekilde gönderilebileceği ve kullanıcılar için daha güvenli bir haberleşme yolu sağlanabileceği söylenebilir.

5.5. AES Algoritması ile Güvenli SMS Gönderme Mobil Uygulama Testlerinin Yorumlanması

Çizelge 5.1’de test sonuçlarında görüldüğü gibi Tekno Spark 6-Go fiziksel cihazı ile iki farklı emülatör yani sanal cihazla yapılan şifreleme ve deşifreleme süreleri açısından karşılaştırıldığında fiziksel cihaz oldukça hızlıdır. Alınan mesaj uzunlukları arttıkça şifreleme ve deşifreleme süreleri de artmıştır. Ancak yine de oldukça hızlıdır. Literatürde de

söylendiği gibi AES simetrik şifreleme algoritmaları donanımsal cihazlarda oldukça hızlıdır. Ek olarak güvenliği ve gücü kanıtlanmış bir algoritmadır. Bu özellikleri ile AES şifreleme algoritması gizli haberleşme gereken askeri, bankacılık, finans, sağlık gibi alanlarda güvenli SMS'de kullanılabileceği yapılan mobil uygulama ve analiz ile gösterilmiştir.

BÖLÜM 6

SONUÇ VE TARTIŞMA

Hızla gelişen teknolojiyle beraber sıklıkla kullanılan mobil haberleşme uygulamalarında güvenli iletişim daha da önemini arttırmaktadır. Mobil haberleşme uygulamalarından biri olan SMS hızlı ve internet gerektirmeyen bir iletişim aracıdır. SMS ile haberleşmede kullanıcılar her ne kadar güvenli iletişim yaptıklarını düşünseler bile SMS mesajının gönderildiği trafiğin dinlenebildiğini, herhangi bir siber saldırı olması durumunda güvenli ve gizli bir iletişimin aksayacağını düşünemezler. İletilen SMS mesajlarının daha güvenli iletilmesi, istenmeyen üçüncü kişilerden korunma gereği gibi durumlarda şifreleme yöntemlerine başvurmak mesajın gizliliği ve bütünlüğü açısından bir çözüm olarak önemli yere sahiptir.

Bu tezde gerçekleştirilen mobil uygulama sonucunda SMS mesajı güçlü ve hızlı AES-256 blok simetrik şifreleme algoritması ve RSA asimetrik şifreleme algoritmasıyla şifrelenmiştir. Şifreleme ve şifre çözme süreleri açısından değerlendirilmiş olup gizlilik ve bütünlük bozulmadan güvenli ve hızlı bir şekilde gönderilebileceği ve kullanıcılar için daha güvenli bir haberleşme olanağı sunabileceği gösterilmiştir. Uygulama gizliliğin önemli olduğu organizasyonlarda, askeri personelin haberleşmesinde, finans sektörlerinde, hasta mahremiyeti için sağlıkta ve gizli bilgi paylaşımının gerektiği birçok yerde kullanılabilir.

Kullanılan şifreleme yöntemleri alanlarında güçlü olduğu için saldırganların şifreli SMS bilgisini çözmeleri zordur. AES algoritması matematiksel olarak kırılma zorluğu güç olan bir algoritma olduğu için kaba kuvvet saldırısına da dayanıklıdır. Ancak gizli anahtar paylaşımının güvenli kanallardan yapılması önemlidir. Bu durumun simetrik şifreler için dezavantaj olduğu söylenebilir. Gizli anahtar paylaşımında sır paylaşım şemalarını kullanmak çözüm olarak düşünülebilir.

RSA asimetrik şifreleme algoritmalarıyla yapılan SMS mesajı gönderme mobil uygulamamızdaki sonuçlara göre güvenli, hızlı bir iletişim sağlanabileceği söylenebilir. RSA algoritmasındaki güvenlik seçilen anahtarın büyüklüğü ile doğru orantılıdır. Çünkü anahtar oluşturmak için seçilen asal sayıların büyük olması saldırganlar için anahtarı elde etmedeki zorlukla sonuçlanır. Ancak bu algoritmada seçilen asal sayıların çok büyük olması fazla işlem gücüne sebep olmaktadır. Dolayısıyla şifreleme ve çözme işlem süreleri AES'e göre daha yavaştır.

Ayrıca seçilen anahtar uzunluğuna ve mesaj uzunluğuna göre SMS mesajlaşma servisi sadece 160 karakterle sınırlı olduğu için şifreleme sonucu elde edilen mesaj daha fazla karakterde olma durumu söz konusu olabilir. Bu durumda mesajı bölerek göndermek ya da sıkıştırma algoritmalarından faydalanmak gerekli olabilmektedir.

Şu anki teknoloji ile AES ya da RSA algoritmalarıyla yapılan şifreli SMS mesajının haberleşme esnasında kırılması mümkün gözükmemektedir. Gelecekte kuantum bilgisayarlar ile birlikte olası bir durum olsa bile bu teknolojilere karşı korunmak için kuantum kriptografi de gelişmektedir.

Sonuç olarak tezin temel amacı olan şifreli bir mobil SMS haberleşmesi ile ayrı ayrı AES ve RSA şifreleme algoritmaları kullanılarak güvenli bir iletişim sağlanabileceği ortaya konmuş ve AES algoritmasıyla gerçekleştirilen uygulama Google play platformunda kullanıcıya sunulmuştur. RSA algoritması ile güvenli SMS haberleşme mobil uygulamamız gerekli iyileştirmelerden sonra Google play platformunda kullanıcıya sunulması hedeflenmektedir.

KAYNAKLAR

Android, (2011). http://developer.android.com/guide/basics/what-is-android.html

Arda, D., & Topaç, Ç. (2020). Secure Sms Application In Mobile Communication. Van Internatıonal Applıed Scıences Congress. July 24-25, 2020 Van, Turkey

Ariffi, S., Mahmod, R., Rahmat, R., & Idris, N. A. (2013). *SMS Encryption Using 3D-AES Block Cipher on Android Message Application*. Advanced Computer Science Applications and Technologies (ACSAT), International Conference on. IEEE.

Architecture, F. (2020). Flutter Architecture. https://www.javatpoint.com/flutter-architecture. sitesinden: 05.01.2023 tarihinde erişilmiştir.

Bodur, H., Kara, R., & Zavrak, S. (2015). RSA Şifreleme Algoritmasını Kullanarak SMS İle Güvenli Şifreleme Yöntemi. XVII. Akademik Bilişim Konferansı. Anadolu Üniversitesi, Eskişehir.

Chavan, R.R., & Sabnees, M. (2012, March). Secured mobile messaging. In 2012 *Internatşonal Conference on Computing , Electronics and Electrical Technologies* (ICCEET) (pp. 1036-1043). IEEE

Çalışkan, H., & Dener, M. (2015). Şifreli SMS gönderimi için Android Tabanlı Mobil Uygulama, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *1*(1), 26-31.

Demirbilek, A. S. (2021). Güvenli Elektronik Seçim İçin Sır Paylaşım Şemalarının Uygulanması. Yüksek Lisans Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

Daemen, J., & Rijmen, V. (1999). AES Submission Document on Rijndael, Version 2, [PDF belgesi]. 10 Ocak 2021 tarihinde http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf adresinden erişildi.

Daemen, J., & Rijmen, V. (2002). The Desing of Rijndal: AES- The advanced encrption standard. Heidelberg: Springer.

Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 469 - 472.

FIBS PUB-197. (2001). Advenced Encryption Standard. [PDF belgesi]. 05.01 2023 tarihinde https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf. adresinden erişildi.

Forouzan, B. A. (2008). *Cryptography and Network Security*. New York, USA: McGraw-Hill Inc.

Fast-Rsa, (2023). https://pub.dev/packages/fast_rsa.

Flutter (2022). Flutter architectural overview. https://docs.flutter.dev/resources/architectural-overview. Sitesinden 05.01.2023 tarihinde erişilmiştir.

GitHub. (2020). *A Small Place to Discover Languages in Github.* https://madnight.github.io/githut/#/issues/2022/2. Sitesinden 05.01.2023 tarihinde erişilmiştir.

Gülcüoğlu, E., Üstün, A. B., & Seyhan, N., (2021), Comparison of Flutter and React Native Platforms, IUYD'2021 / 12(2)

ITU (International Telecommunication Union). (2010). "The World in 2010". https://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf sitesinden 05.01.2023 tarihinde erişilmiştir.

Kalenderi, M., Pnevmatikatos, D., Papaefstathiou, I. & Manifavas, C. (2012). Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-end FPGAS. 22nd Field Programmable Logic and Applications (FPL) Conference, 747-753, Oslo.

Kılınç, D. (2013). http://denizkilinc.com/android-isletim-sistemi-mimarisi-kernel-libraries-runtime-framework-dvm/ sitesinden 06.01.2023 tarihinde erişilmiştir.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics Of Computation*, 203-209.

Kodaz, H., & Botsalı, F. M. (2010). Simetrik Ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması, *Selçuk-Teknik Dergisi*.9(*1*) 10-23

Marketing-Türkiye (2022). https://www.marketingturkiye.com.tr/haberler/kisa-mesajin-tarihi/ 05.01.2022 tarihinde erişilmiştir.

Muştu, Y., & Çavuş E. (2012). *Kısa Mesaj Sunucu Tasarımı*. ELECO. Bursa.

Muştu, Y. (2012). Sms Ve Android Tabanlı Uygulamalarla Sınıf İçi Etkileşimin Arttırılması, Yüksek Lisans Tezi, Bilecik Üniversitesi, Fen Bilimleri Enstitüsü, Bilecik.

Open Handset Alliance, (2011). http://www.openhandsetalliance.com/oha_members.html.

Peersman, G., Griffiths, P., Spear, H., Cvetkovic, S., & Smythe, C. (2000). *A tutorial overview of the short message service within GSM.* Computing & Control Engineering Journal , 79-89.

Peersman C., Cvetkovic S., Griffiths P. & Spear H. (2000). The global sys- tem for mobile communications Short Message Service. *IEEE Personal Communications,7*(3)15-23

Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 120-126.

Stinson, D.R. (2002). Cryptography : Theory and Practice. Second Adition, New York: CRC/C&H.

Solit net. (2022). https://soltik.net/android-ve-ios-kullanim-oranlari-aciklandi/. Nisan 2022 tarihindeki yazısından. 08.01.2023 tarihinde erişildi.

Taç, M. (2011). *Android Programlama*. Dikeyeksen,İstanbul.

Tüfekçi, M. (2018). AESX+, AESX, AES-128 ve AES-256'nın Performans ve Güvenlik Açısından Karşılaştırılması. Ege Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.

Yayla, R., Üçgün, H., & Tunçer, S. (2020). A Research on Encryption Methods and Account Security, 8 th International Symposium on Innovative Technologies in Engineering and Science, Volume 3, Issue 1, Pages: 385-394, DOI :10.33793/acperpro

Yuksel, M.E. & Zaim, A.H. (2009). Sending multilingual SMS on GSM/GPRS devices", Proceedings of the 11th Academic Information Conference, pp. 229-238.

Webtekno. (2022). Flutter Nedir, nasıl kullanılır? https://www.webtekno.com/flutter-nedir-nasil-kullanilir-h115673.html. sitesinden 05.01.2023 tarihinde erişilmiştir.

ÖZGEÇMİŞ

1997 yılında Tekirdağ'ın Çorlu ilçesinde doğdu. Lise öğrenimini Çorlu ilçesi Mehmet Rüştü Uzel Mesleki ve Teknik Anadolu Lisesi'nde tamamladı. 2019 yılında Trakya Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nden mezun olarak lisans eğitimini tamamladı. Çalışma hayatına 2019 yılında Trakya Üniversitesi Teknopark bünyesinde özel bir şirket ile Bilgisayar Mühendisi olarak başlayan yazar halen bu görevi yürütmektedir.

TEZ ÖĞRENCİSİNE AİT TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER

Uluslararası Hakemli Kongrede Sunulan ve Yayınlanan Bildiri

Arda, D, & Topaç, Ç. (2020). Secure Sms Application In Mobile Communication. Van International Applied Sciences Congress. July 24-25,Van, Turkey